DOWNLOAD PDF CONSUMER ELECTRONICS LEARNING MODULE.

Chapter 1 : Consumer Electronics Servicing NC II | Nhoerj Lorenzana - www.nxgvision.com

Welcome to the world of Consumer Electronics Servicing!This Module is an exploratory course which leads you to Consumer Electronics ServicingNational Certificate Level II (NC II)1.

The security parameters comprise an encryption key used for encryption of communications over the network. The device comprises an entry device that enable a user to input the security parameters comprising at least an encryption key used for an encryption of communication over a wireless network. The security parameters are stored in a memory arrangement. The security parameters may then be further transmitted to the new device via an infrared signal respecting security parameters. The invention also relates to control devices and more particularly to bi-directional remote controllers that can be easily reconfigured or re-loaded with new data. The invention also pertains to security over wireless networks and more particularly to a way connected devices of the network can learn of security parameters associated with the network. Home networking has become a growing area of the consumer electronic industry. Wireless standards such as IEEE Each device needs to be installed on the network and needs to acquire knowledge of the network characteristics before it can communicate and exchange data and control information with other devices on the network. To that respect, reference is made to patent document US 6,,, incorporated herein by reference, that describes a network system with Plug-and- Play capability where a controller gets an abstract representation of a new device on the network describing the modality to control a specific functionality of the device. Wireless data communications need to be protected from deliberate corruption or eavesdropping at a much higher level than wireline communications and advance is made into this direction in most WLAN or WPAN to protect communications. For example, IEEE WEP is an encryption mechanism that takes the content of a data frame and passes it through an encryption algorithm using a variable length encryption key, the WEP key. The WEP key is known by both the encrypting and the decrypting stations. A first mechanism is to set a default key, which is shared by all stations in the secured network. A second mechanism allows a station to establish a "key mapping" relationship with another station. An advantage of the second mechanism over the first one is that the fewer stations possessing the key, the less likely the key will be revealed. However the first mechanism enables any station to communicate securely with all other stations in the network. A station may therefore independently communicate over each of the various secure overlapping wireless networks using different sets of security parameters respecting the various WLANs. Each set of security parameters may be stored in respective network profiles that the station can retrieve when needed. Reference is made to co-pending U. This document discloses a system for determining whether a user device may communicate in a detected wireless network based on profiles of security parameters of the device. If it is determined that one of the profiles of the device contains the right security parameters for the detected network, then the user is notified and the device is enabled, and may even be configured, to communicate over the network. Thus, for a station to communicate over a secure network, it needs to learn of the encryption key or any other security parameter necessary to secure communication over the network. Network privacy issues may imply advanced set up and specific configuration of the device that can easily become a burden or a discouraging task for a non-expert user. The inventor has realized that there is a need for an easy and secure way of configuring a new device to operate over a network. It is an object of the invention to provide a system that permits easy, fast and reliable configuration of new devices in secured networks. It is another object of the invention to advantageously use existing IR capability of some consumer electronic devices for installation of these devices over a wireless network. To this end, a system of the invention comprises an entry module for enabling inputting a set of security parameters comprising at least an encryption key for encryption of communication over a wireless network. The device also comprises a storage arrangement for storing the set of security parameters and an infrared emitter. The device communicates to a first infrared-controllable apparatus an infrared signal respecting the set of security parameters for set-up of a second apparatus over the wireless network. The invention further relates to a method for installing a controllable apparatus in a wireless network and communicating the set of security parameters to the apparatus via an infrared signal. A device of

the invention is loaded with the security parameters so that it can further convey these parameters to the first apparatus via infrared. In an embodiment, the first and the second apparatuses may actually be one apparatus and in such case the apparatus, which is installed on the wireless network has IR capability. Alternately, the first and second apparatuses are connected to each other, via wireless or wireline link, and the first apparatus, which receives the set of security parameters, may convey these to the second apparatus. A device of the invention may be a conventional learning remote controller such as the Pronto currently manufactured by Philips. Such a remote controller may be configured to control any device in the home by loading into it new data and new command codes that the controller uses to generate new control commands. Thus, the remote controller may be loaded with the security parameters so that these, especially the encryption key, can be further transmitted to apparatuses that are controllable through IR commands. IR technology can be easily implemented at a reasonable price and most consumer electronic devices are manufactured with built-in IR capability. Advantage is therefore taken in the invention of the widespread of IR technology to enable IR-controllable apparatuses to learn of security parameters specific to a wireless network. One or more embodiments of the invention therefore provide an easy way to install devices on a secure wireless network that have both wireless capabilities to communicate over a wireless network and built-in IR-capabilities. The invention is explained in further details, by way of examples, and with reference to the accompanying drawing wherein: Elements within the drawing having similar or corresponding features are identified by like reference numerals. The invention relates to an installation process for initial set up of a new device on an existing wireless network. In order for the device to communicate over the network, it needs to acquire the security parameters in use on the network. For example, such security parameters comprise an encryption key used by stations of the network to secure communications. This encryption key may be a bit key, a key generation algorithm or an encryption pattern. In the invention, advantage is taken of the fact that the device that will be installed on the network has IR-capability. If the device does not have the right IR- capability advantage is taken of the fact that the device may communicate with another device that has IR-capability. Such device is, for example, a set-top box, a television, a stereo system at home that is conventionally controlled through IR commands from a remote controller or any device in the home that is connected via a wireless or a wireline link to another IR-capable device. In the installation process of the device on the network, the remote controller is loaded with the security parameters respecting the wireless network. The remote controller is for example temporarily connected to the access point of the network, which transmits the parameters to the remote controller in a secure fashion. The remote controller may also be connected to a trusted device of the wireless network such as a personal computer to which the access point is connected. The remote controller, which is configured to control the device via IR commands, may then easily communicate the security parameters to the device. This installation process may be rendered feasible by the download on the remote controller of a software application, which enables the remote controller to receive the security parameters and which further enables the remote controller to convey these security parameters to the device through modulation of an IR signal. The remote controller may further configure the device to recognize the transmitted security parameters as such. Station may be a device in the home such as a stereo system. This embodiment is described hereinafter in the context of the installation of device onto network Device has built Device is, for example, a personal entertainment set-top box pre-equipped with an embedded wireless module, of which only antenna is shown, that will enable device to receive digital audio and video content from another station or the access point in the home once device is installed onto network Device may be controlled via remote controller through IR control commands. To this end, controller and device respectively comprise IR modules and with both IR sensors and transmitters enabling controller and device to receive and transmit IR modulated coded data. Controller may be a bi-directional controlling device that can be set-up to control new devices and new functionalities. Controller can be set in a learning mode in which controller can receive new data and new control code from which controller is configured to generate new control commands. A more detailed embodiment of controller is shown in Fig. Processing unit may have the minimum required processing power to process incoming IR signals and process user inputs to effect changes by generating IR signals. In another embodiment, controller may also comprise a display and processing unit

may comprise additional processing power to process audio and video data, e. Controller may also be a cellular phone or a personal digital assistant with built-in IR and loaded with a software application that enables it to control devices and learn new control commands. In this embodiment, network is an IEEE It must be noted that the invention encompasses any type of wireless network other than IEEE Any station desiring to communicate over network needs to first acquire the security parameters associated with network and more particularly the WEP key currently in use. In this embodiment the WEP key is initially set up by access point and is known by both access point and station already installed onto network In the invention, the user inputs the security parameters into device by means of controller as will be explained as follows. As mentioned previously, the set of security parameters respecting network is currently known by access point and station Device may thus get the security parameters from either access point or station In another embodiment, the user may directly enter the security parameters and the WEP key into controller via a user interface or a keyboard coupled with or of the controller In this embodiment, security parameters are communicated to device from access point via infrared signals. Access point comprises a bi-directional infrared module Controller is temporarily set in a learning mode, in which mode controller is configured to receive new data, e. Once in the learning mode, controller is placed so that the IR sensor of module is in the emitting range of module The user then initiates the transfer of security parameters from access point to controller Controller stores the received security parameters in memory Processing unit , or memory , may have been previously loaded with a software application that enables the transfer of the security parameters from access point to device according to the invention. Controller may be configured to store the security parameters specific to network in a more secure fashion than controller typically stores codes for regular control commands so that security parameters cannot be easily hacked from controller In addition, the security parameters may be further encrypted before modulation over IR when transmitted from access point to device for increased security. This embodiment as shown in Fig. Upon transmission to controller , processing unit controls the storage of the security parameters into memory Controller is thereafter set in a control mode, in which controller can transmit information data and control commands to other devices in the home. As mentioned earlier device has an IR module comprising an IR sensor. Controller is placed so that the IR transmitter is placed in the receiving range of IR sensor of module The user may then initiate the transfer of an IR signal representative of the security parameters stored in memory to device Module generates the signal by modulation of IR rays with the security parameters. To that respect, reference is made to US 5,, of the same assignee, hereby incorporated by reference. This document discloses a remote control system for transmitting messages whose length is adapted to the nature of the operating command and the quantity of information to be transmitted. It must be noted that the security parameters may be sent as a macro from and to controller A macro is a pre-programmed series of commands sent from a first device to a second device to operate the second device. Thus, depending on the IR protocol used, controller may have to send more than one command to transfer security parameters as a macro. Device may be configured to automatically recognize security parameters including the WEP key from the received IR signal. Alternately in another embodiment, the user may have to preset device to indicate that the IR signal received from controller includes security parameters respecting network

Chapter 2 : Modules - Learning Modules for an Electronics Curriculum

CONSUMER ELECTRONICS SERVICING 2 K to 12 - Technology and Livelihood Education Welcome to the world of Consumer Electronics Servicing! This Module is an exploratory course which leads you to Consumer Electronics.

This document attempts to provide an entry to the world of consumer electronics troubleshooting and repair. It also covers test equipment selection, tools and supplies, parts, home made troubleshooting aide - Incredibly Handy Widgets tm - and safety. Mostly, you will learn by doing. However, you do need to prepare. There are many schools dedicated to electronics repair. Some of these are quite good. This document, however, is written from the perspective of the motivated do-it-yourselfer, hobbiest, and tinkerer. The Repair FAQs usually list suggested references for each area. Your local public or university library will probably have some of these or other repair oriented electronics books. Above all read and understand the document: Your life may depend on it. Collect broken electronics and appliances from your friends, relatives, the dump, garage sales and flea markets, etc. Start on those that have been written off - you will screw up at first. As times passes, your batting average will improve. It may not happen overnight but it will happen if you apply yourself. Sometimes, the basic design is flawed or someone before you messed up royally. Troubleshooting is like being a detective but at least the device is generally not out to deceive you. Experience will be your most useful companion. If you go into the profession, you will obtain or have access to a variety of tech tips databases. These are an excellent investment where the saying: However, to learn, you need to develop a general troubleshooting approach - a logical, methodical, method of narrowing down the problem. A tech tip database might suggest: This is good advice for a specific problem on one model. Therefore, in many cases, some reverse engineering will be necessary. As always, when you get stuck, the sci.

Chapter 3 : Arduino RFID: Consumer Electronics | eBay

Consumer electronics learning module 1. Republic of the Philippines DEPARTMENT OF EDUCATION K to 12 Basic Education Curriculum Technology and Livelihood Education Learning Module CONSUMER ELECTRONICS SERVICING EXPLORATORY COURSE Grade 7 and Grade 8.

The security parameters comprise an encryption key used for encryption of communications over the network. The device comprises an entry device that enable a user to input the security parameters comprising at least an encryption key used for an encryption of communication over a wireless network. The security parameters are stored in a memory arrangement. The security parameters may then be further transmitted to the new device via an infrared signal respecting security parameters. The invention also relates to control devices and more particularly to bi-directional remote controllers that can be easily reconfigured or re-loaded with new data. The invention also pertains to security over wireless networks and more particularly to a way connected devices of the network can learn of security parameters associated with the network. Home networking has become a growing area of the consumer electronic industry. Wireless standards such as IEEE Each device needs to be installed on the network and needs to acquire knowledge of the network characteristics before it can communicate and exchange data and control information with other devices on the network. To that respect, reference is made to patent document US 6,,, incorporated herein by reference, that describes a network system with Plug-and- Play capability where a controller gets an abstract representation of a new device on the network describing the modality to control a specific functionality of the device. Wireless data communications need to be protected from deliberate corruption or eavesdropping at a much higher level than wireline communications and advance is made into this direction in most WLAN or WPAN to protect communications. For example, IEEE WEP is an encryption mechanism that takes the content of a data frame and passes it through an encryption algorithm using a variable length encryption key, the WEP key. The WEP key is known by both the encrypting and the decrypting stations. A first mechanism is to set a default key, which is shared by all stations in the secured network. A second mechanism allows a station to establish a "key mapping" relationship with another station. An advantage of the second mechanism over the first one is that the fewer stations possessing the key, the less likely the key will be revealed. However the first mechanism enables any station to communicate securely with all other stations in the network. A station may therefore independently communicate over each of the various secure overlapping wireless networks using different sets of security parameters respecting the various WLANs. Each set of security parameters may be stored in respective network profiles that the station can retrieve when needed. Reference is made to co-pending U. This document discloses a system for determining whether a user device may communicate in a detected wireless network based on profiles of security parameters of the device. If it is determined that one of the profiles of the device contains the right security parameters for the detected network, then the user is notified and the device is enabled, and may even be configured, to communicate over the network. Thus, for a station to communicate over a secure network, it needs to learn of the encryption key or any other security parameter necessary to secure communication over the network. Network privacy issues may imply advanced set up and specific configuration of the device that can easily become a burden or a discouraging task for a non-expert user. The inventor has realized that there is a need for an easy and secure way of configuring a new device to operate over a network. It is an object of the invention to provide a system that permits easy, fast and reliable configuration of new devices in secured networks. It is another object of the invention to advantageously use existing IR capability of some consumer electronic devices for installation of these devices over a wireless network. To this end, a system of the invention comprises an entry module for enabling inputting a set of security parameters comprising at least an encryption key for encryption of communication over a wireless network. The device also comprises a storage arrangement for storing the set of security parameters and an infrared emitter. The device communicates to a first infrared-controllable apparatus an infrared signal respecting the set of security parameters for set-up of a second apparatus over the wireless network. The invention further relates to a method for installing a controllable apparatus in a wireless

network and communicating the set of security parameters to the apparatus via an infrared signal. A device of the invention is loaded with the security parameters so that it can further convey these parameters to the first apparatus via infrared. In an embodiment, the first and the second apparatuses may actually be one apparatus and in such case the apparatus, which is installed on the wireless network has IR capability. Alternately, the first and second apparatuses are connected to each other, via wireless or wireline link, and the first apparatus, which receives the set of security parameters, may convey these to the second apparatus. A device of the invention may be a conventional learning remote controller such as the Pronto currently manufactured by Philips. Such a remote controller may be configured to control any device in the home by loading into it new data and new command codes that the controller uses to generate new control commands. Thus, the remote controller may be loaded with the security parameters so that these, especially the encryption key, can be further transmitted to apparatuses that are controllable through IR commands. IR technology can be easily implemented at a reasonable price and most consumer electronic devices are manufactured with built-in IR capability. Advantage is therefore taken in the invention of the widespread of IR technology to enable IR-controllable apparatuses to learn of security parameters specific to a wireless network. One or more embodiments of the invention therefore provide an easy way to install devices on a secure wireless network that have both wireless capabilities to communicate over a wireless network and built-in IR-capabilities. The invention is explained in further details, by way of examples, and with reference to the accompanying drawing wherein: Elements within the drawing having similar or corresponding features are identified by like reference numerals. The invention relates to an installation process for initial set up of a new device on an existing wireless network. In order for the device to communicate over the network, it needs to acquire the security parameters in use on the network. For example, such security parameters comprise an encryption key used by stations of the network to secure communications. This encryption key may be a bit key, a key generation algorithm or an encryption pattern. In the invention, advantage is taken of the fact that the device that will be installed on the network has IR-capability. If the device does not have the right IR- capability advantage is taken of the fact that the device may communicate with another device that has IR-capability. Such device is, for example, a set-top box, a television, a stereo system at home that is conventionally controlled through IR commands from a remote controller or any device in the home that is connected via a wireless or a wireline link to another IR-capable device. In the installation process of the device on the network, the remote controller is loaded with the security parameters respecting the wireless network. The remote controller is for example temporarily connected to the access point of the network, which transmits the parameters to the remote controller in a secure fashion. The remote controller may also be connected to a trusted device of the wireless network such as a personal computer to which the access point is connected. The remote controller, which is configured to control the device via IR commands, may then easily communicate the security parameters to the device. This installation process may be rendered feasible by the download on the remote controller of a software application, which enables the remote controller to receive the security parameters and which further enables the remote controller to convey these security parameters to the device through modulation of an IR signal. The remote controller may further configure the device to recognize the transmitted security parameters as such. Station may be a device in the home such as a stereo system. This embodiment is described hereinafter in the context of the installation of device onto network Device has built Device is, for example, a personal entertainment set-top box pre-equipped with an embedded wireless module, of which only antenna is shown, that will enable device to receive digital audio and video content from another station or the access point in the home once device is installed onto network Device may be controlled via remote controller through IR control commands. To this end, controller and device respectively comprise IR modules and with both IR sensors and transmitters enabling controller and device to receive and transmit IR modulated coded data. Controller may be a bi-directional controlling device that can be set-up to control new devices and new functionalities. Controller can be set in a learning mode in which controller can receive new data and new control code from which controller is configured to generate new control commands. A more detailed embodiment of controller is shown in Fig. Processing unit may have the minimum required processing power to process incoming IR signals and process user inputs to effect changes

by generating IR signals. In another embodiment, controller may also comprise a display and processing unit may comprise additional processing power to process audio and video data, e. Controller may also be a cellular phone or a personal digital assistant with built-in IR and loaded with a software application that enables it to control devices and learn new control commands. In this embodiment, network is an IEEE It must be noted that the invention encompasses any type of wireless network other than IEEE Any station desiring to communicate over network needs to first acquire the security parameters associated with network and more particularly the WEP key currently in use. In this embodiment the WEP key is initially set up by access point and is known by both access point and station already installed onto network In the invention, the user inputs the security parameters into device by means of controller as will be explained as follows. As mentioned previously, the set of security parameters respecting network is currently known by access point and station Device may thus get the security parameters from either access point or station In another embodiment, the user may directly enter the security parameters and the WEP key into controller via a user interface or a keyboard coupled with or of the controller In this embodiment, security parameters are communicated to device from access point via infrared signals. Access point comprises a bi-directional infrared module Controller is temporarily set in a learning mode, in which mode controller is configured to receive new data, e. Once in the learning mode, controller is placed so that the IR sensor of module is in the emitting range of module The user then initiates the transfer of security parameters from access point to controller Controller stores the received security parameters in memory Processing unit , or memory , may have been previously loaded with a software application that enables the transfer of the security parameters from access point to device according to the invention. Controller may be configured to store the security parameters specific to network in a more secure fashion than controller typically stores codes for regular control commands so that security parameters cannot be easily hacked from controller In addition, the security parameters may be further encrypted before modulation over IR when transmitted from access point to device for increased security. This embodiment as shown in Fig. Upon transmission to controller , processing unit controls the storage of the security parameters into memory Controller is thereafter set in a control mode, in which controller can transmit information data and control commands to other devices in the home. As mentioned earlier device has an IR module comprising an IR sensor. Controller is placed so that the IR transmitter is placed in the receiving range of IR sensor of module The user may then initiate the transfer of an IR signal representative of the security parameters stored in memory to device Module generates the signal by modulation of IR rays with the security parameters. To that respect, reference is made to US 5,, of the same assignee, hereby incorporated by reference. This document discloses a remote control system for transmitting messages whose length is adapted to the nature of the operating command and the quantity of information to be transmitted. It must be noted that the security parameters may be sent as a macro from and to controller A macro is a pre-programmed series of commands sent from a first device to a second device to operate the second device. Thus, depending on the IR protocol used, controller may have to send more than one command to transfer security parameters as a macro. Device may be configured to automatically recognize security parameters including the WEP key from the received IR signal. Alternately in another embodiment, the user may have to preset device to indicate that the IR signal received from controller includes security parameters respecting network

Chapter 4 : Allegro MicroSystems - Camera Modules

Consumer Electronics Learning Module Uploaded by Nick Bantolo This Module is an exploratory course which leads you to Consumer Electronics Servicing National Certificate Level II (NC II)1.

Chapter 5 : Consumer electronics - Wikipedia

This Learning Module was developed for the Exploratory Courses in Technology and Livelihood Education, Grades 7 and 8 of the K to 12 Curriculum with the assistance of the following persons: This Learning Module on Consumer

DOWNLOAD PDF CONSUMER ELECTRONICS LEARNING MODULE.

Electronics Servicing NC II was developed by the following personnel: MODULE WRITERS MARCELO E. TAN, Ed. D. EPS 1, DepED.

Chapter 6 : Car Security Keys & Transponders in Consumer Electronics for sale | eBay

This Module is an exploratory course which leads you to Consumer Electronics Servicing National Certificate Level II (NC II)1. It covers five common competencies that a Grade 7 / Grade 8 Technology and Livelihood Education (TLE) student like you ought to possess, namely.

Chapter 7 : Troubleshooting and Repair of Consumer Electronic Equipment

The Module is designed to be a teacher-assisted learning kit or a self-learning kit on competencies that a Grade 7 TLE ought to possess. It explores the course on Consumer Electronics Servicing which helps your student earn a Certificate of Competency in Grade 9which leads to a.

Chapter 8 : What are Consumer Electronics (CE)? - Definition from Techopedia

The authors gratefully acknowledge the sponsorship of the National Science Foundation. The work described in this paper was funded by grants from the Department of Undergraduate Education - through the Course, Curriculum and Laboratory Instrumentation (CCLI) Educational Materials Development program (DUE - and DUE -).

Chapter 9 : Download: Technology and Livelihood Education (TLE) Grade 10 TGs and LMs â€“ SanayGuro

Grade 10 LMs and TGs for TLE subjects are available here! Download Technology and Livelihood Education (TLE) Teaching Guides (TGs) and Learner's Materials (LMs) for Grade 10 from the links below.