UgCERT
UGANDA COMPUTER EMERGENCY RESPONSE TEAM

UGANDA COMMUNICATIONS COMMISSION

Small Office/Home Office Router Security

Introduction

Home routers have become an integral part of our modern society as our use of the internet has grown to include business from home, school work, social networking, entertainment and personal financial management. Wired and now wireless routers have moved into our homes to facilitate this additional connectivity. The internet service provider (ISP) sells these devices pre configured and ready to use. Users typically connect immediately to the internet without performing any additional configuration. They may not know how to perform additional configuration because it either seems too difficult, or they may be reluctant to spend the time with advanced configuration settings.

Unfortunately, the default configuration of most home routers offer little security and leave home networks vulnerable to attack. Small businesses and organizations that lack the funding for an information technology (IT) infrastructure and support staff often use these same home routers to connect to the internet. These organizations frequently also set up the routers without implementing security precautions and therefore are exposing their organization to attack.

Security Concerns

The default configurations of most home routers offer little security. Home routers are directly accessible from the internet, are easily discoverable, are usually powered-on at all times, and in many cases are vulnerable due to misconfiguration. These characteristics offer an intruder the perfect attack vector. The wireless features incorporated into many of these devices adds another vulnerable attack vector.

Mitigation

The mitigation steps listed below are designed to increase the security of home routers and reduce the vulnerability of the internal network against attacks from external sources.

- Change the default login username and password: Manufacturers set default usernames and passwords for these devices at the factory to provide users access to configure the device. These default usernames and passwords are readily available in different publications and are well known to attackers; therefore, they should be immediately changed during the initial router installation. A strong password that uses a combination of letters and numbers with 14 characters or more is recommended. Furthermore, change passwords every 30 to 90 days.

- **Change the default SSID:** A service set identifier (SSID) is a unique name that identifies a particular wireless LAN (WLAN). All wireless devices on a WLAN must use the same SSID in order to communicate with each other. Manufacturers set a default SSID at the factory that typically identifies the manufacturer or the actual device. An attacker can use the default name to identify the device and any vulnerability associated with it. Users sometimes set the SSID to a name that identifies their organization, their location, their own name, etc. This makes it easier for the attacker to identify their specific business or home network based upon an SSID easily identified with their name. For example, an SSID that broadcasts a company name is a more attractive target then a router broadcasting "ABC123". When choosing an SSID, follow the best practices policy for password complexity as described below:
    - The minimum length of an SSID should be greater than eight characters long.
    - Use alphanumeric and symbols in the SSID.
    - Change the SSID on a reoccurring basis and discourage the use of previous
    - passwords.

- **Configure WPA2-AES for data confidentiality:** Wireless Equivalent Privacy (WEP) is a security algorithm intended to provide data confidentiality (authentication and encryption) but has serious weaknesses. WEP was superseded by the 802.11 standard implemented as Wi-Fi Protected Access (WPA), which has a newer version, WPA2. WPA and WPA2 provide stronger authentication and encryption using dynamically changing keys. WPA and WPA2 come in personal and enterprise versions. WPAPersonal, also referred to WPA-PSK (Pre-Shared Key), was designed for homes and small offices using pre-shared keys without requiring an authentication server. If using WPA-PSK, set a long pre-shared key and change it periodically. WPA-Enterprise requires a RADIUS authentication server, uses Extensible Authentication Protocol (EAP), and provides added security, but it entails a larger budget and more complicated implementation. WPA2 incorporates AES 128-bit encryption accepted by government agencies. WPA2 with AES represents the most secure option, and all wireless devices must be WPA2 compliant. If WPA2 is not feasible, WPA is an alternative. WEP represents the least secure option. If used, WEPshould be configured with the 128-bit key option with the longest pre-shared key the router administrator can manage.

- **Limit WLAN coverage:** LANs are inherently more secure than WLANs because they are protected by the physical structure in which they reside. WLAN coverage frequently extends beyond the perimeters of your home or organization. This allows eavesdropping by intruders outside yournetwork perimeter. Therefore, antenna placement, antenna type, and transmission power levels are important aspects to consider. Limit the broadcast coverage area whensecuring your WLAN. A centrally located omni-directional antenna is the most commontype used. If possible, use a directional antenna to direct WLAN coverage to only the areas needed. Experimenting with transmission levels and signal strength will also limit the coverage to only the areas needed.

- **Turn the network off when not in use:** The ultimate in wireless security measures, shutting down the network, will most certainly prevent outside attackers from breaking in. While it may be impractical to turn the devices off and on frequently, consider this approach during travel or extended periods offline.

- **Disable UPnP:** Universal Plug and Play (UPnP) is a handy feature allowing networked devices to seamlessly discover and establish communication with each other on the network. Though the UPnP feature eases initial network configuration, it is also a

security hazard. For example, malware within your network could use UPnP to open a hole in your router firewall to let intruders in. Therefore, disable UPnP when not needed.

- **Upgrade firmware:** Just like software on your computers, the router firmware (the software that operates it) must have current updates and patches. Many of the updates address security vulnerabilities that could affect the network.

- **Use static IP addresses or limit DHCP reserved addresses:** Most home routers are configured as Dynamic Host Configuration Protocol (DHCP) servers. DHCP makes configuration of client devices easy by automatically configuring their network settings (IP address, gateway address, DNS info, etc.). However, this also allows unauthorized users to obtain an IP address on your network. Disabling DHCP and configuring clients manually is the most secure option, but it may be impractical depending on the size of your network and support staff. If using DHCP, limit the number of IP addresses in the DHCP pool. It may limit the number of users, potentially including unauthorized users, that can connect to your network.

- **Disable remote management:** Disable this to keep intruders from establishing a connection with the router and its configuration through the wide area network (WAN) interface.

- **Disable remote upgrade:** This feature, if available, allows the router to listen on the WAN interface for TFTP traffic that could potentially compromise the router firmware. Therefore, it should be disabled.

- **Disable DMZ:** The router's demilitarized zone (DMZ) creates a segregated network exposed to the internet, used for hosts that require internet access (web servers, etc.). Disable this feature if not needed. Users or administrators sometimes enable it for troubleshooting reasons and then forget to deactivate it, exposing any system inadvertently placed there. A firewall is recommended if this feature is used.

- **Disable unnecessary services:** As with any computer system, disable all unnecessary services in order to reduce the router’s exposure.

- **Disable ping response:** The ping response setting is usually disabled by default. With this feature enabled, reconnaissance on the router becomes easier then when it is disabled. It allows your router to respond to ping commands issued from the internet, and it potentially exposes your network to intruders. Although disabling this feature will not shield you from discovery, it will at least increase the difficulty of discovery. Verify that the service is disabled.

- **Enable router firewall:** Most home routers include an internal firewall feature. Ensure this feature is activated and carefully configured to allow only authorized users and services access to the network. Activate stateful packet inspection (SPI) on your firewall if it is an available function. SPI extends firewall capability by inspecting packets to distinguish legitimate traffic from unsolicited traffic. Another feature offered by many home routers is the creation of whitelists or blacklists to allow or disallow a list of websites, services, ports, etc. Take advantage of this feature if it is available. Note that the firewall built in to the router does not prevent wireless users within range of your wireless network from connecting to it.

- **Logging:**Enable router logging and periodically reviewthe logs for important

information regarding intrusions, probes, attacks, etc.

- **Monitor the wireless traffic:** Monitor the wireless traffic to identify any unauthorized use of your network by performing routine log reviews of the devices that have accessed the router. If an unknown device is identified, then a firewall or MAC filtering rule can be applied on the router. For further information regarding how to apply these rules, see the literature provided by the manufacturer or the manufacturer's site.

- **Administrator workstations:** Verify that any administrator workstation used to manage the router is on a trusted segment of the network to mitigate outsiders sniffing the management data and collecting information about your network.

- **Disable bridging and use network address translation (NAT):** Home routers separate the internal network from the internet using network address translation (NAT). NAT provides private IP addresses for all the devices on your network. It is not directly accessible from the internet, nor can discovery of the network's internal addresses be accomplished easily. The IP address of the external interface of the router conceals the devices on your network that are behind it. This adds an additional layer of security.

- Some routers include a feature that allows them to act as a bridge between two networks. This feature can be used to connect segments or devices on the same intranetto the internet using a routers routable IP address. Disable this feature if not required, to further limit the attack surface of the router.

Keep in mind, this is only a list of suggested steps that can potentially help secure your small office or home router. Employing some of these suggested steps may not be feasible in your network or your environment. If further assistance is required, see your router manufacturer's literature.