iSmartGuard

One-Stop Solution for Protecting Wi-Fi Enabled Devices

iSign International

Setting up small business and home networks is a relatively simple concept. However, simplicity can mean that users may choose to set up their devices heedlessly and consequently leave their data vulnerable to hacking attempts. Read on to know how iSmartGuard protects all Wi-Fi enabled devices from the adversaries.

The tools and techniques used by hackers are rapidly growing in numbers and types, with cyber adversaries coming up with innovative ideas to steal our sensitive and confidential data every day. One of the most widely preferred ways of hacking among malicious actors is Wi-Fi hacking. There are mainly of two types of Wi-Fi Hacking- one in which the hacker intercepts the Wi-Fi to connect their device, which is often referred to as MITM (Man-In-The-middle) attack. The second, which is more dangerous, in which the Wi-Fi network is hacked, compromising the connected devices, and taking complete control of them.

The Inherent Weaknesses in Wi-Fi Networks

Any wireless device can become a soft target for hackers. Wi-Fi hacking is easier than hacking a device connected to that Wi-Fi. There are many tools that adversaries use to breach the less secure Wi-Fi routers. Apart from this, there are also advanced tools that can even breach a Wi-Fi router with high security. In general, every access point on a Wi-Fi network has the potential for hacking.

Routers with WEP security are the easiest to hack. Synonymous with home networks, WEP is a type of encryption algorithm used to secure the wireless connection. However, organizations these days secure the routers with WPA-PSK keys, which are tough to hack, but this does not mean that these are unhackable.

The most common mistake that many users do is using the default Wi-Fi password. Hackers can use the default password to gain unauthorized access to the Wi-Fi connection and gain access to connected devices.

There are several ways to protect the home/organizational network and devices from malicious minds.

- Changing the default Wi-Fi network names (SSIDs) and passwords.
- Enabling firewall for added security in the devices
- Updating the firmware of all Wi-Fi-enabled devices, routers, and other hardware regularly.
- Deploying device security apps like iSmartGuard by iSign International.

Scenarios That Enable Adversaries to Attack Wi-Fi Networks

Wi-Fi is standard in spaces like public libraries, homes, and small businesses such as insurance companies and banks. The latter are generally far from the reach of the central information technology (IT) department. Thus, they may find it cumbersome to enforce compliance with company network policies. Moreover, monitoring the remote office locations can be tricky for the IT pros as they may be on network segments, which are different from those of the rest of the company.

Individuals who introduce their Wi-Fi routers enabled with WEP into their companies' networks, may also effectively present the risk of attacks into the structures. Thus, companies or institutions can be subject to network compromise.

The motivations of attackers vary.

- They may break into corporate networks to gain unauthorized access to data.
- They can aim to hijack vulnerable routers and other networked devices to turn these into parts of botnets.
- Attackers can launch further attacks from compromised devices, the most notorious of which are the distributed denial-of-service (DDOS) attacks.

- Some professional attackers even go as far as removing traces of their activity to make post-infection forensics even more difficult.

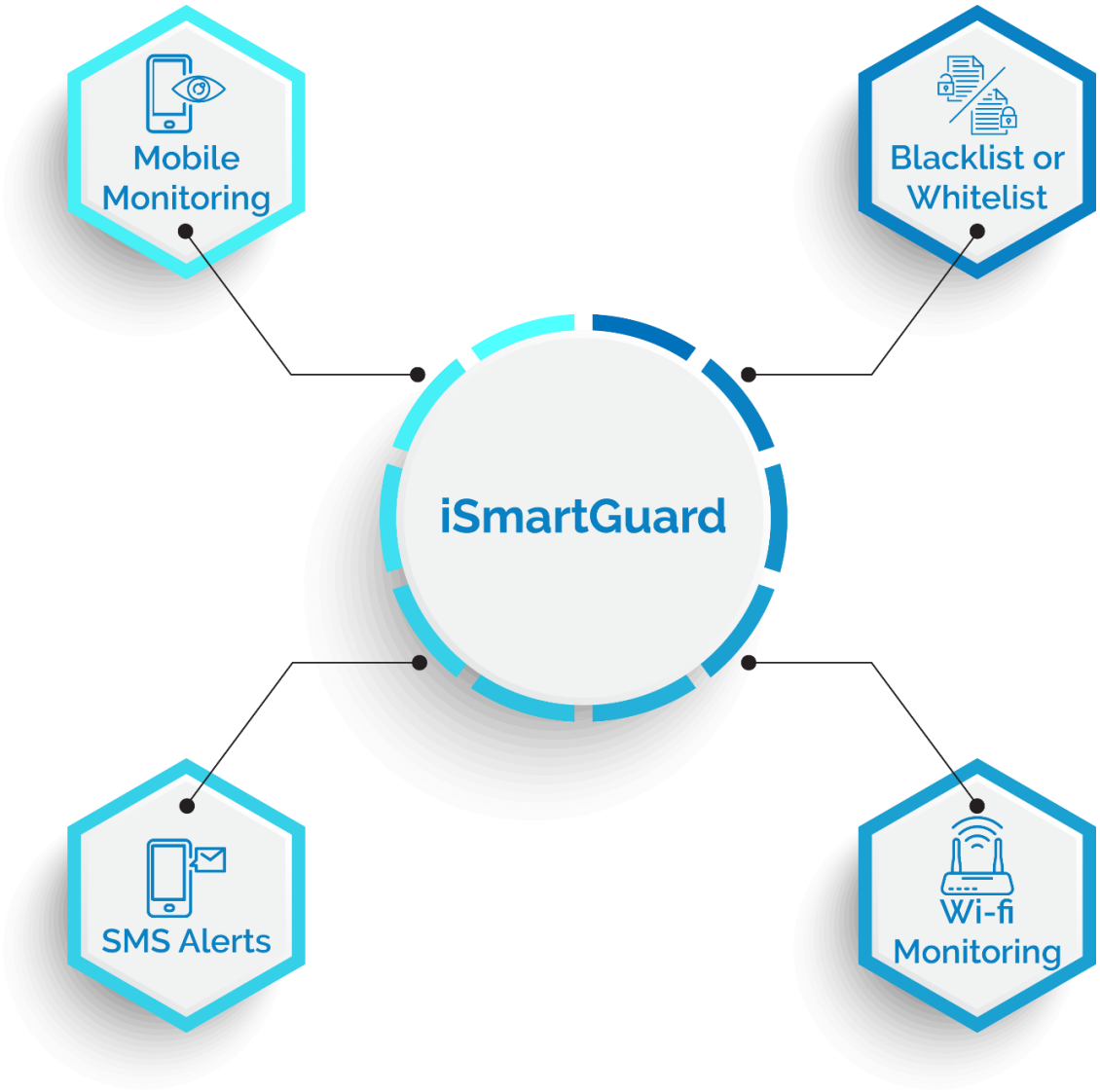
These attacks can happen without the knowledge of the network owners and devices.

iSmartGuard – An Unbreakable Cyber Security Shield for Wi-Fi Enabled Devices

iSmartGuard by iSign International is a desktop and mobile application designed to monitor, block & remove intruders. The app is suitable for individual users, small businesses, and universities alike. It ensures that the connections on the Wi-Fi network are trusted, and users can remove any malicious ones. All iSign Products come with 6-factor authentication.

Features

- **Mobile Monitoring:** No matter where they are, users can manage their iSmart Guard and iSmart Guard M.
- **Blacklist or Whitelist:** These lists quickly block unwanted ISPs and their associated IP Addresses. It helps users to remove unwanted intruders instantly.
- **SMS Alerts:** Users get a text message when the threats reach set levels.
- **Monitoring All Wi-Fi Enabled Devices:** Users can monitor all equipment linked to Wi-Fi. They can easily review the activities of their Wi-Fi-enabled devices



3rd Party Validation

Arizona State University's Center for Cybersecurity and Digital Forensics carried out a study to determine the effectiveness of iSmart Guard against internal or external hacking of Wi-Fi enabled devices such as laptops, computers, and Internet-Of-Things devices. An analysis of all devices was preformed to determine which connections were genuine after two weeks of use. They were, therefore, "whitelisted" as authorized. All other links were blocked.

It was determined that iSmartGuard was 100% efficient in blocking all unauthorized connections while allowing only authorized ones.

Conclusion

It is evident from the discussion that there are existing vulnerabilities in Wi-Fi security protocols and hardware components introduced by manufacturers. iSign's iSmartGuard is an innovative which helps monitor and detect malicious activities in real-time by leveraging hardware-assisted security assurance for home and business environments. To learn more visit our website at https://isigninternational.com/.