CONNECTED HOME SECURITY

Consumer Technology Association (CTA)™ Whitepaper

Consumer Technology Association™

DISCLAIMER

CONSUMER TECHNOLOGY ASOCIATION (CTA)™ CONNECTED HOME SECURITY WHITEPAPER

The Document is for general information and is designed to delineate subjects and procedures for consideration. Information contained in this Document should not be used without first obtaining competent professional or technical advice with respect to its suitability in any given situation. CTA does not warrant or assume any liability or responsibility for the accuracy, completeness or usefulness of any information contained in this Document. CTA disclaims any and all warranties, express or implied, that such information is suitable for any general or particular use and that cited information is non-infringing upon a third party's intellectual property rights. Anyone making use of this document assumes all liability resulting from such use.

The existence of the document does not in any respect preclude a CTA member or nonmember from manufacturing, selling, or installing products not conforming to the document, nor does its designation as a CTA document preclude its voluntary use by persons other than CTA members. This document does not purport to address all security issues or all applicable regulatory requirements. It is the responsibility of the user of the document to establish appropriate security practices and to determine the applicability of regulatory limitations before use of the document.

CTA reserves the right to change, revise, add to, or delete any data contained in this document without prior notice.

TABLE OF CONTENTS

Introduction 3
Passwords 4
- Password Guidelines 4
- Sources and More Information 5

Networking 6
- Networking Guidelines 6
- A/V Components 7
- About Encryption 7
- Sources and More Info 7

Modems and Routers 8
- Separate Devices 8
- Once You Have Selected The Router 8
- Sources and More Information 9

Consumer Network Management Tools and Devices 10
VPNs – Virtual Private Networks 10
- VPN Guidelines 10
- Sources and More Information 10

Z-Wave/ZigBee 11
- Overview 11
- Basic Z-Wave Network Security 11
- Enhancing Z-Wave Network Security with AES 128 12
- Basic ZigBee Network Security 12

NFC – Near Field Communication 12
- NFC Risk 12
- Sources and More Info 12

Bluetooth 13
- Bluetooth Precautions 13

Home Security Systems / Access Control 13
- Home Security Systems 13
- Access Management 13
- Security Cameras 14

Mobile Devices 14
- During Installation 14
- After Mobile Device is Stolen 14

Documentation / Credential Stewardship 15
A final word: Maintenance 15
Glossary 16
About the Consumer Technology Association (CTA)™ 17

INTRODUCTION

This Connected Home Security Whitepaper is intended to do the following:

1) Outline existing best practices, standards and methods that are reasonable solutions to current and forthcoming smart home security challenges. The scope includes the system components, IoT devices and other products consumers install themselves or have professionally installed that may be considered consumer technology.

2) Help make the end user's connected home system more secure by providing enhanced protection against hacking and other networks, IOT, or smart home/connected home related threats.

3) Reduce potential exposure of professional installers by providing an industry approved guide installers/integrators can use as a tool to ensure they are providing reasonable and effective measures to protect their installed systems against current and emerging malware attacks and "bad actors" (hackers).

4) Create "value-add" for the new IoT marketplace and ecosystem through:

- Accredited advice by licensed and professional tradespersons
- Documented recommended practices or processes for selecting products, system(s),installation and maintenance
- Sharing of additional resources for more secure and reliable system installations

Utilizing the latest best practices can provide enhanced security, reliability, and enjoyment for IoT owners and users; and provide more upgradable professional Residential installations.

WHO SHOULD USE THIS GUIDE

This document is intended for the professional tradesperson. This group includes integrators, alarm contractors and others involved in the professional installation and maintenance (moves/adds/changes) of smart home systems and components.

PASSWORDS

Passwords are often the first (sometimes the only) line of defense against intrusion and hacking.

Password Guidelines

Most of the recommendations in this section are adapted from Symantec's website, please see http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices for the full article.

- Always change default USERNAMEs and PASSWORDS. Never leave the "factory default" password. Also, changing the "factory default" username increases the difficulty of hacking a router.
- What NOT to use
  - **No Dictionary Words, Proper Nouns, or Foreign Words, No Personal Information, No regular words with numbers at ends**
  - Password should not include anything remotely related to the user's name, nickname, or the name of a family member or pet.
  - For home networking, the home address or anything related is a poor choice.
- What TO do
  - ALWAYS change the factory or initial password on any device.
  - NEVER leave the default password in place.
  - It is often suggested to change this before even plugging a device into the network, thus preventing hacking before the password is changed.
- How to create a strong password - **Length, Width and Depth**
  - **Length** – Hackers have automated the process of guessing a password. The longer a password, the more difficult it is to guess—longer is better. It is generally recommended that passwords be between six and nine characters. *(Note, between eight to fifteen characters is increasingly being recommended to offset increased hacker capabilities.)*
  - **Width** - As a general rule the following character sets should all be included in every password:
    - Uppercase letters such as A, B, C
    - Lowercase letters such as a, b,c
    - Numerals such as 1, 2, ...
    - Special characters such as $, ?, &; and alt characters such as µ, £, Æ.
  - Depth - Depth refers to choosing a password with a challenging meaning – something not easily guessable. Phrases and things easy to remember but hard to guess.
- Should biometrics (for example, fingerprint technology) be available, this may be easier than passwords for many customers.
- Passwords should be updated periodically; preferably quarterly. Consider including this in service and maintenance agreements.
- Use a trusted password management1 system to store and change passwords for the client. This document should be at minimum hidden, and at best encrypted. Follow-up with clients periodically, preferably quarterly, on password maintenance.
- When researching and selecting a password management system, explain that you are a professional technician and will need to maintain passwords on behalf of your client; preferably the system should have an option to delegate password maintenance to you on the client's behalf.
- When hints are required for recovery of passwords, consider that many hints, such as "mother's maiden name", use information that is easily discovered elsewhere on the Internet by bad actors. Be selective with hints that are familiar and unique to the client.

- Use different passwords for all devices and systems. Use a different administrative password for client modems, routers, switches and devices. Never share passwords across devices or across clients.
- For client passwords that you cannot control, consider requiring the client to be physically present and able to enter the password for you each time it is required during the installation and setup. Do not accept responsibility for client passwords unless you can make them strong and maintain them.
- Setup a guest Wi-Fi network in addition to the client's Wi-Fi network, so you and your clients are not giving out the Wi-Fi password to every guest to the home. A second (Guest) network is typically included in today's routers. If a Guest network feature is not included in the router, consider adding a second access point with a separate Wi-Fi network for guest usage.

Sources and More Information

- http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
- http://security.fnal.gov/UserGuide/password.htm
- http://www.pcmag.com/article2/0,2817,2407168,00.asp
- https://www.grc.com/passwords.htm

NETWORKING

Networking Guidelines

- Network security does not eliminate the need for computer security. Computers in the home should have up-to-date anti-virus and anti-malware tools installed and running.
- Computers or other networked devices should not run with administrative privileges unless specifically required.
- Limit access from outside the physical structure of the client site.
  - Reduce Wi-Fi power (dB) if possible.
  - Don't provide wired network access (plug-in network port) outside the building.
  - If using power line modem technology, investigate ways to block or firewall the signal for outdoor power (mains) outlets. (Such blocking/filtering/firewalling technologies vary with power line technology type.) Segmenting the network
  - Consider separate segments for different purposes, such as home office, home entertainment, and gaming. Each of these segments has a different security posture and different assets to protect.
  - Segments can be designed using
    - VLANs
    - VPNs
    - Separate physical cabled networks
    - Separate Wi-Fi channels
- For hardwired networks (non-wireless)
  - Pros:
    - Visibility, it is possible to see the physical cable plugged into the network
    - Doesn't advertise the existence of the network over RF
    - Provides a higher barrier to radio-based hacking ("sniffer" attacks). Such attacks are still feasible, but far more difficult with cabled systems.
    - Guaranteed data bandwidth
  - Cons:
    - Difficulty of installation
- Basic security setup
  - Take a snapshot of the "as built" configuration. Over time, comparing snapshots will show new devices. Automated tools such as Fing (from Overlook) can help with "as built" and "as maintained" configuration and change tracking.
  - Static vs DHCP
  - MAC address use, etc.
  - Devices - passwords, usernames, secure setup (utilize a password manager that is capable of dual management)
- Gaming – If the customers include gamers and may be hosting games
  - Consider a separate network segment for gaming (see "Segmenting the network", above)
  - Note that this is one of the instances where enabling UPnP on the Internet ("WAN") side of the router may be required. When UPnP is visible from the Internet, instead of blocked on the Internet side of the router, it can provide additional paths for hackers to enter the system.
- Wi-Fi - securing a Wi-Fi network, what not to do, what to do
  - Use a network DMZ with care, if at all, as the DMZ is by definition a less secure portion of the installed network. A typical DMZ opens all ports and connects to a designated LAN device or computer, or server.
  - Always use password encryption. Never leave Wi-Fi open without a password. Use WPA2-Personal with AES (preferred) or WPA2-Personal with TKIP.2
  - Change default SSIDs

- Turn off SSID Broadcasting
- Disable WPS (Wi-Fi Protected Setup); a hacker can brute-force guess the PIN in a few hours
- Consider Wireless MAC Filtering on older products when no other choices are available to enhance security, but be aware that MAC Filtering can be spoofed.
  Newer product should have more options than this.
- Use Network monitoring app to see what devices are using your network
- Setup a Guest Network with a separate SSID, password protection and logoff timers.
- The 5.0 GHz band may help to limit distance and who can see the network, although it is not guaranteed.

A/V Components

Note that many A/V components, such as high-end AVRs and smart TVs, have integrated networking capabilities just like computers and routers. Treat these devices as important parts of the installed network, and apply the security guidance here to these devices as well.

About Encryption

Encryption can provide a significant level of protection from unauthorized viewing, changes, or access to sensitive data by encoding it and requiring a password or key to unlock it for viewing, changes, or access. In Residential environments encryption is often available in many products to provide more security for the user but is rarely enabled by default.

2 Other options are WEP and WPA (as compared to WPA2). WPA is not considered as safe as WPA2. WEP is older and has been considered obsolete for a number of years; a Wi-Fi installation protected with WEP can be hacked quickly using commonly available tools.

Enabling encryption can provide better system protections but can also potentially complicate interoperability and integrations. Enabling encryption may also degrade system performance as encryptions' extra protection often engenders some performance degradation. Consider the use of authentication vs. full encryption where performance and security are priorities and it is available. Authentication prevents unauthorized access but lacks the full privacy protections of encryption.

Sources and More Info

- http://www.pcmag.com/article2/0,2817,2409751,00.asp
- http://www.linksys.com/us/support-article?articleNum=136993
- http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/
- http://www.howtogeek.com/173921/secure-your-wireless-router-8-things-you-can-doright-now/

MODEMS AND ROUTERS

Separate Devices

- The Modem translates the cable or fiber signal from outside the home, to a single Ethernet path inside the home. The Router makes this Ethernet path available to all the authorized devices in the home.
- ISPs typically provide a box that combines the Modem and Router functions in one; it will have a connector for the cable or fiber from the street, and RJ45 connectors and Wi-Fi to attach to consumer devices.
- This bundled approach is convenient but may not be the most secure way. The box provided by most ISPs is distributed by the millions; such volume makes it an attractive target for hackers. If the consumer is using an ISP-provided bundled solution, check to see if the ISP is updating the box firmware ("push" updates).
- To take control of this situation, install a separate aftermarket Router and maintain it for the consumer. Keeping up with aftermarket firmware updates is a high-maintenance approach, but the same router is likely suitable for most customers. However, the bundled ISP device needs to have a "bridge" mode to pass traffic to an aftermarket Router. Without a "bridge" mode, you cannot connect an aftermarket Router to the ISP's bundled Modem+Router.
  >> Note, not all ISPs' boxes have a "bridge" mode.
- Commercial-grade routers are more expensive than consumer routers, but have additional options for protection, Quality of Services (QoS), intrusion detection, Gateway anti-malware and Gateway anti-spam.

Once You Have Selected The Router

- Immediately download and install the most up-to-date firmware for the router. If possible, do this on a relatively trusted network rather than in the customer's home. Or, use open source alternatives such as Tomato or DD-WRT (note that these are examples only; also that open source alternatives do not have the same level of support as aftermarket products).
- Remove/Disable common Router threats
  - Change default admin username AND password. Use a strong password (see Passwords section)
  - Turn off Remote Administration of the router.
  - Disable UPnP on the router. UPnP allows applications to request port mapping to computers on the other side of the router, creating a security risk.
  - Disable HNAP; this remote management protocol is not considered to be secure (for example, it is vulnerable to a man-in-the-middle attack).
  - Turn off WPS on the router. See also other important Wi-Fi configuration steps in the Networking Guidelines.
- Use the customer router's Firewall
  - Block all ports, then unblock the ports used by the consumer's applications. Because ports can be assigned to applications, it is not possible to pre-define the "safe" ports. However, few non-technical customers are typically using things like FTP (port 21) or TelNet. On the other hand, they will need port 80 for http and port 443 for https.
  - After blocking most ports, set a notification when a connection attempt on a blocked port has been made (how to set such a notification is firewall-specific). The notification will help trace any blocked ports that should be unblocked, and also will indicate when someone is trying to gain remote access through the firewall.
  - For additional security, where possible use non-standard port values on applications, and open those on the firewall instead of the standard port values. For example, use the FTP application settings option to change the FTP app to use port 8021 instead of 21.
- Use a VPN Router/Service to encrypt all data going out of your network. (See "VPNs – Virtual Private Networks")
- If port forwarding in the router is required for remote access, manage this for security purposes. Try to keep such remote access on a separate network segment, for example; or use in combination with a VPN.

- Consider partnering with a vendor that provides additional network security, engineering and support. Turn off any unused services/ports, so others cannot gain access thru them.
- Use a port scanning tool like nmap to check the private network (that is, the portion behind the firewall, also called the subnet). Confirm that the services found are actually necessary. The Internet Assigned Numbers Authority maintains a website with ports and services (see http://www.iana.org/assignments/service-names-port-numbers/service-names-portnumbers.xhtml). There are also port scanning services available.
- For all devices on the home network (subnet), check and update device software or firmware regularly or set for automatic updates from the manufacturer
- Logout of Admin services when done configuring a router. Some do not auto-log-out.

Sources and More Information

- https://www.sans.org/security-resources/policies/network-security/pdf/router-andswitch-security-policy
- http://www.computerhope.com/issues/ch001289.htm
- http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554
- http://www.tomsguide.com/us/home-router-security,news-19245.html
- https://www.grc.com/shieldsup
- http://www.tripwire.com/state-of-security/vulnerability-management/wireless-routervulnerabilities-leave-enterprise-networks-vulnerable/
- http://www.routerpwn.com/ (list of known router vulnerabilities and checks)
- https://nvd.nist.gov/ (National Vulnerabilities Database)
- http://www.iana.org/assignments/service-names-port-numbers/service-names-portnumbers.xhtml
- http://lifehacker.com/198946/how-to-portscan-your-computer-for-security-holes

CONSUMER NETWORK MANAGEMENT TOOLS & DEVICES (CNMDS)

Consumer Network Management Tools and Devices (CNMDs) minimize risks of unwanted network intrusion by blocking and limiting access to certain websites, portals and VPNs. CNMDs also allow filtering of access to the Internet via time scheduling, IP address, and MAC address. Some CNMDs may include parental control management, allowing management of what network devices connect to what Internet sites and when access is allowed. CNMDs come in a variety of flavors and forms but most CNMDs are hardware devices with built-in software, but software-only versions are also available.

- Use CNMDs to supervise, limit access to, and guard the network against hackers
- Setup CNMDs to manage access to suspicious social networks, search engines and websites
- Setup every network device (IP camera, thermostats, door locks, personal computers), including all IoT devices, to limit access to only updates and necessary data
- Setup every media device (ie. streaming media players) to limit access to media, firmware and update websites only
- Establish guidelines and update settings within the CNMD setup pages to protect the network against infiltration via malware and ransomware pushes

VPNS – VIRTUAL PRIVATE NETWORKS

VPN's are typically used for remote access solutions in the Residential environment. Virtual Private Networks can be used to augment the security both LAN and WAN data traffic from eavesdropping, interception, or manipulation.

VPNs can protect user data by wrapping it in a layer of encryption and protecting user data from unauthorized 3rd parties and provide privacy for sensitive communications.

VPN Guidelines

- VPNs can be added to many Residential networking environments with either new hardware ("VPN appliance") or may even be an unused feature of some existing SOHO installations.
- VPNs can also be installed on the Residential LAN with a hosted "cloud" server
- VPNs can be provided in a variety of protocols and products. Some examples include
  - TLS / SSL (note that SSL is considered insecure and obsolete, and that TLS 1.2 is recommended)
  - PPTP
  - L2TP
  - IPSEC
  - OpenVPN
- For remote access a TLS VPN should be used to provide secure access.

Sources and More Information

- http://www.smallbusinesscomputing.com/testdrive/article.php/3501156/VPN-Gateway-Appliances--Access-Remote-Data-Like-the-Big-Guys.htm

Z-WAVE/ZIGBEE

Overview

Z-Wave and ZigBee Residential products are both examples of low bandwidth, meshnetworking, radio frequency (RF) radio technologies used in a Local AREA Network (LAN) to enable the Internet of Things (IOT). However, although both Z-Wave and ZigBee are both meshnetworking technologies, these are separate and distinct technologies that operate in the sub GHZ, 900 MHZ band or 2.4 GHZ radio spectrum in the NA market (USA, Canada, and Mexico).

Z-Wave or ZigBee are existing technologies and may be already be in customers' homes forming a hidden, but potentially vulnerable connection point in the Residential environment. When installing new Z-Wave or ZigBee products or networks try to identify any existing, potentially compatible products to ensure they are documented, secured, and can be leveraged for meshnetworking as required.

Both Z-Wave and ZigBee products typically wirelessly connect "peer to peer" and/or to a Wide Area Network (WAN) Residential gateway, security system, AV electronics, or other Residential CE networking devices.

Network typologies vary, but mesh-networking products have become more popular in the Residential market and should be properly secured against accidental or unauthorized usage without a user's consent or knowledge. Communicating ZigBee or Z-Wave Residential devices can include thermostats, lighting controls, door locks, shades, and other popular CE products or embedded home electronics that form the basis of increasingly popular home automation and energy management systems. Both Z-Wave and ZigBee technologies often connect to iOS and Android mobile electronics (such as smartphones and tablets), and interface to cloud services for Residential customers and remote access.

Z-Wave mesh-networking products operate in the sub-GHZ, 900 MHZ band and are primarily deployed in Residential single family homes or apartments for communicating with and controlling AV, Energy management, lighting, thermostats, sensors, and other home electronics. When installing Z-Wave devices the following is recommended to secure properly and maintain a Z-Wave mesh network.

Basic Z-Wave Network Security

Note and document the 4Byte "Home ID" of an installation's primary controller. This 4Byte code is a very important and confidential number to retain and not share. This code is the unique identifier for a particular Z-Wave network. The Home ID is required to participate in the Z-Wave network; if a new device doesn't know the Home ID, it cannot communicate on the ZWave network. The same is true of malicious attackers. Therefore, if a Home ID is compromised (disclosed outside the owner's control) it should be regenerated at the primary controller, in order to create a new, unique Home ID.

Existing Home ID's should not be "recycled" to simplify installations in different structures or homes.

Although Z-Wave is a relatively short range (30' average), it is often possible to set a lower RF power rating to minimize signal leakage from a residence. If this enhanced privacy is desired, this can be accomplished by increasing the density of the mesh-network with additional products and lowering the respective RF signal strength of each device.

Make sure that Network related functions (such as commissioning and decommissioning) are Password protected and are not triggered automatically, but triggered based on action of Network's administrator,

Enhancing Z-Wave Network Security with AES 128

In additions to the Home ID above, some Z-Wave devices employ an enhanced AES 128 cryptographic key for supplementary authentication to operate sensitive applications such as access control devices such as door locks and garage doors. In the unlikely event that a Z-Wave device's AES 128 key is compromised, it can be regenerated in addition to a new Home ID.

Basic ZigBee Network Security

ZigBee networks can be secured by the AES-based CCM* security suite, assuming the products themselves support the feature. A few points to consider are:

- Leaving the ZigBee network disconnected from the Internet is safest. However, this eliminates any remote management option.
- If the ZigBee network must be connected to the Internet, ensure that the only device connected to the Internet is the ZigBee gateway and that there is a firewall between the gateway and the rest of the network.
- Filter Internet traffic entering and leaving the ZigBee network by address (source and destination) and port number. Don't allow unrestricted traffic to flow between the ZigBee network and the rest of the world.
- If the option for 802.15.4 security features exists in the ZigBee products, enable it. There are two levels of security, one at the 802.15.4 (lower) level and one at the network+application (higher) levels. Enabling both kinds of security is more secure.
- Know the function of the ZigBee Coordinator. This is a feature within (most likely) the ZigBee router. It is the encryption key manager and application configuration manager. Some products specifically call themselves the Coordinator; others only mention it in the user guide or specification sheet. However, the Coordinator is the most critical component requiring protection—physical and otherwise—in the ZigBee network.

NFC – NEAR FIELD COMMUNICATION

NFC Risk

NFC works via wireless signals over a very short range, typically a few centimeters. Because of this short range, the design of NFC discourages security issues. NFC chips need an NFC reader device to power them up. However, in general NFC technology does not offer protection against eavesdropping attacks, making it important for consumers and businesses to take preventative physical security measures.

- For the professional installer, the primary concern is ensuring that NFC readers, whether for building access or other purposes, are not situated or mounted as to allow for easy "sniffing" or for easy tampering.
  - Sniffing: Data interception can be done if the hacker can install additional electronics in very close proximity. Ensure the reader is in a visible, well-lit and uncluttered space.
  - Tampering: Hardware can be tampered with; ensure the hardware is securely mounted in such a way as to be tamper-resistant.

Sources and More Info

- http://www.nearfieldcommunication.org/nfc-security-risks.html
- http://www.makeuseof.com/tag/using-nfc-3-security-risks-to-be-aware-of/
- http://www.forbes.com/sites/michaelvenables/2013/08/08/wall-of-sheep-near-fieldcommunication-hack-at-def-con/

BLUETOOTH

Bluetooth is a short range, typically "point to point" protocol that is used for communications, command and control in a variety of CE products. Typically Bluetooth is limited in range to 30'. Bluetooth can be used to stream audio (A2DP), to command and control AV (AVRCP), to create local hotspots, and to perform other bridging functions for clients to a LAN and/or WAN and in a wide variety of Residential or mobile CE products.

Bluetooth is marketed under several version levels:

- Bluetooth (prior to Bluetooth 4.0) is the original line of Bluetooth protocols, suitable for audio, networking and control.
- Bluetooth Low Energy (or Bluetooth LE or simply BLE) is a new protocol under the same trademark "Bluetooth" banner. BLE is best suited for short, occasional bursts of data from a battery-powered node, such as a wireless thermometer or fitness device. While not capable of the speed of the faster Bluetooth protocol, it consumes far less power. BLE devices frequently have no encryption or security features.
- Bluetooth 4.0 combines the two protocols, the original higher-speed Bluetooth options and the lower-power BLE.

Bluetooth Precautions

- Bluetooth protocol is considered reasonably secure, and the short range limits attackers to those physically present.
- Bluetooth products often feature encryption (128 Bit) and/or authentication mechanisms for enabling and using connections. Enable these security features when possible.
- Use "non-discoverable" options where available.
- Bluetooth low energy (BLE) devices broadcast a beacon signal, be aware these beacons are visible to other Bluetooth devices and should not contain sensitive information such as full names, physical addresses, etc.

HOME SECURITY SYSTEMS / ACCESS CONTROL

Home Security Systems

- Dealers should maintain an internal policy on system activation, testing and turn over.
- At the time of activation, request the client to change Master Code without revealing to Dealer/Installer.
- Leave as part of the client package, clear instructions on how to change/manage Master and Users Codes.
- Dealers only maintain "Installer Codes" which are not capable of disarming the system.
- Clients' requests for Dealer to manage Codes should be done in writing. A responsibility and limited liability agreement is recommended.
- Dealers who offer Security Monitoring should take reasonable steps to protect monitoring agreements that contain client information including verbal passcodes.

Access Management

- As with Home Security Systems (see above), dealers should maintain an internal policy on system activation, testing and turn over.
- Dealers should be aware of codes relating to fail safe or fail secure methodologies for both residential and commercial applications.
- Clients should be provided instructions on how to change/manage Administrator and User codes, view access logs.
- Clients' requests for Dealer to manage Codes should be done in writing. A responsibility and limited liability agreement is recommended.
- For systems that use a card or chip for access, periodic audits should be performed to assure the devices are still in the possession of outside trades and service providers.

Security Cameras

- As with Home Security Systems and Access Management (see above), dealers should maintain an internal policy on employee access and their user rights, password management, testing and turn over.
- Dealers should be aware of applicable state and local codes relating to public and private use applications along with any required postings or notifications to occupants. This applies to video and audio functionality as these features may have different code requirements.
- Clients should be provided instructions on how to change/manage Administrator and User access codes.
- Clients' requests for Dealer to manage Codes should be done in writing. A responsibility and limited liability agreement is recommended.
- For systems that provide alerts upon device failure or tampering, notifications should be properly set up and tested.
- It is recommended that non-standard Internet ports be used for remote viewing. Note also that enabling remote viewing does carry some risk of hackers gaining access to the video stream. Sensitive (private) locations should not be enabled for remote viewing if possible.
- Set record quality and overwrite rules to suit user needs for both visual performance and length of storage.
- Confirm night view performance.
- Use adequate back up power source for DVR and Cameras when possible.

MOBILE DEVICES

This section considers what to do if a customer loses their phone.

There are various levels of protection to ensure your mobile phone does not fall into the hands of someone who can then get control of your home system. The precautions below should be considered for all phone and tablets of each person in the home.

During Installation

- Use a cell phone password: First, with all the accounts your phone can access, one should protect the phone with a password to get into the phone. This is the first level of protection.
- Don't let the system save passwords: If you have a choice of saving the password or requiring a password to log into your home system, always choose to require the password each time you log in.
- Have a second method: Ensure your connected home system can enable, disable and change your passcode to your system. This way if you do lose your phone you can change your remote log-in passcode.
- Limit access: Some control systems will allow you to choose what you can access remotely. One can disable access to certain features as an extra level of protection. For example, limit access to cameras from kids' phones.
- Include the rest of the family: Share these practices with your children and make sure they do not share the passcode with friends.

After Mobile Device is Stolen

- Change the passcode: If your phone auto-connects to the network, change the encryption passcode of your home wireless network so the phone won't auto-connect.

DOCUMENTATION / CREDENTIAL STEWARDSHIP

- Educate clients on the purpose and advantages of remote access.
- Include written authorization in client contracts for the company and its authorized staff to access client's network and its connected devices for the sole purposes of performing services provided by company.
- Develop a "Client Network Access Policy" and make it part of your client orientation. It will build trust if your clients know that they are developing a relationship with someone who understands these threats and is proactively implementing a best practices approach.
- Develop a "Client Network and Device Access Agreement" and make it part of your employment agreements/ documents to be shared at the time of hire and orientation.
- At the time of hire, educate employees on the responsibilities and liabilities of remote and local access to client's networks and its connected devices. Employees need to understand this exposure is not limited to just owners.
- With the use of app's, Internet accessible camera's represent one of the largest liability risks to integrators and their staff. Develop and implement strict policies for access to client cameras and DVR/NVR systems.
- If you offer managed service agreements, include authentication updates as part of the service offering.
- Avoid standardized passwords or password schemes that can be easily shared or abused, post-employment.

A FINAL WORD: MAINTENANCE

A secure installation starts getting less secure as soon as the installer walks out the door, as the customer adds and changes the install, as software upgrades and changes, and as hackers evolve. Of course, the silver lining in this cloud is that there are opportunities for services for the integrator. Security maintenance may not be the most appealing service to offer, unfortunately. Opportunities to track breach attempts on the consumer's network or other attempts on the installation, should be brought to the consumer's attention when possible.

Concerning firmware updates, keeping every device in the installed system updated would be ideal. However, this level of hands-on maintenance may not be feasible within the scope of the installer's business. Note, however, that the router—as the first point of entry from the Internet—is a critical device to keep up-to-date. Other elements of the in-home system may be more or less vulnerable to attack when the hacker is physically on the premises, but the router is potentially vulnerable worldwide.

There is a media cycle for product hacking, coinciding with the summer hacker conferences held annually. Consumers are slowly becoming more aware that their home networks are at risk and are reminded with urgent headlines on a regular basis. Each business is different, but it is hoped that these tips will help the installer build a more secure relationship with customers.

GLOSSARY

Bad Actor	A hacker operating with malicious intent, attempting to break into a protected system.
Cracking (passwords)	Seeking to guess a password, possibly by brute force, social engineering, or other methods.
Demilitarized Zone	A portion of the installed network that operates under less security to allow more risky activity without exposing private (non-DMZ) assets to the risk. DMZs are used to allow a secure corporate network to provide public-facing assets like a public server.
DMZ	*See Demilitarized Zone*.
Encryption	The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. [Source: Wikipedia]
IoT	See Internet of Things.
Internet of Things	A broader definition of the Internet, beyond computers, tablets, smartphones and other more "computer-like" devices, which includes connected devices such as remote sensors, door locks, home appliances and security systems. In the Internet of Things, many existing devices take on new capabilities by becoming connected to the Internet and reachable by manufacturers, developers, cloud service providers and consumers.
Mesh Networking	A networking system of topology and protocols where individual nodes communicate with each other and cooperate in carrying data traffic to and from clients.
Social Engineering	Using people and their natural reactions to human interaction to help penetrate systems. An example might be calling a service provider, pretending to be one of their authorized users, and pleading with the customer service representative to give out private information on that user.

ABOUT THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association (CTA)™ is the trade association representing the $377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies - 80 percent are small businesses and startups; others are among the world's best known brands - enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® - the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

CONSUMER TECHNOLOGY ASSOCIATION (CTA)™
1919 S. Eads St.
Arlington, VA 22202

Tel: 866-858-1555 or 703-907-7600
Fax: 703-907-7675

MARKET RESEARCH AND LIBRARY
Tel: 703-907-7763
Fax: 703-907-7769
info@CTA.tech

STANDARDS AND TECHNOLOGY
standards@CTA.tech
Find CTA online at CTA.tech.