The Transmitter

Published Exclusively for Emergency 24, Inc. Dealers www.emergency24.com Spring 2015

Understanding EMERgency24 Account Numbers

EM24 has recently seen an increase in misprogrammed dialers.

As such, below are a few tips and reminders about account numbers to help ensure the programming is performed correctly so your subscribers are protected.

1. Account numbers are 6-digits, the first two characters are numbers or letters that indicate the line card. The next four digits are the account numbers. (Example: LC-#### means that LC is the line card and #### is the account number/code being transmitted.)

2. When programming a panel for EM24 accounts, you should program the last 4-digits into the dialer or communicator. The exceptions would be a DMP panel sending to a DMP receiver or an account sending 3+1 format:

A) For DMP, you should program the last five digits.

B) 3+1 accounts must have an account number where the third character is zero (Example: LC-0xxx). If the account does not have a zero as the third digit, it cannot use 3+1 format.

3. For each digital dialer line card, there is a Primary and Backup phone number available. If the line card designation is different, then the phone numbers are different. Make sure you are using the correct phone number for that line card.

Continued on Page 3

Hacking and Jamming Issues Hurt the Value of Contracts

Stop investing in vulnerable technology & develop a strategy to recoup what you've already lost.

by Patrick Devereaux, Sr. Vice President

The value of your subscriber contracts may be vanishing before your eyes if you have been installing wireless burglar alarms. In fact, hackers have already figured a way to break into and jam a wireless burglar-alarm system — enabling the perpetrator to easily create false alarms, monitor the activities of the homeowners and disarm the system.

The hack was featured on a recent episode of ABC's Good Morning America, exposing the unsecure nature of radio messages between wireless sensors and the alarm panel. As a result, subscriber contracts for systems with vulnerable hardware are worth much less than before, as any buyer would then need to install new hardware or be legally liable for their decision not to do so.

Inside the Vulnerability

A decade or so ago, the equipment needed to hack an alarm system as shown on the Good Morning America segment would have cost tens of thousands of dollars — and it would have needed to be loaded on a large rack installed in close proximity to the wireless burglar-alarm system it was targeting. Today, with the explosion in technological advancements, a burglar's "tool kit" now includes electronics — including Software Defined Radios (SDRs), which now come free with the purchase of a $20 antenna to connect to a laptop computer. Now, any video gamer can go online to purchase an SDR, which comes with alarm-hacking instructions to mimic the tricks seen on Good Morning America.

But GMA is not the only one talking about this issue. In July 2014, Forbes Magazine ran a feature story, that covered the topic in detail — even listing specific brands of vulnerable hardware, including some of the most commonly used devices available today. Additionally, the topic was featured at the 2014 Black Hat Briefings, a computer security conference that brings together a variety of people interested in information security.

At Black Hat, two researchers — Logan Lamb, a security researcher at the Oak Ridge National Lab and Silvio Cesare of Qualys — separately looked at top-selling wireless home alarm systems. Lamb looked at three top brands of home alarm systems installed by ADT, Vivint and a third unidentified company; Cesare looked at several popular systems used in his home of Australia.

Using simple tools, they proved the alarms can be disarmed, suppressed or even create multiple false alarms that would then make the system seem unreliable. The alarm-hacking presentations were given to representatives of government agencies and corporations,

Continued on Page 2

Continued from Page 1: Hacking and Jamming Issues Hurt the Value of Contracts

representatives of government agencies and corporations, as well as expert hackers who attended the conference. Lamb was the one featured in the GMA segment — where he demonstrated to the world how to exploit two different weaknesses in a typical sensor radio: single-frequency transmission and unencrypted messages. These weaknesses allow both jamming and spoofing (hacking), which is mimicking of a signal from the system.

Jamming occurs when a radio is used to broadcast a stronger signal than the targeted sensor using the same frequency. The result is that no communication from that sensor to the alarm panel is possible. Lamb used an SDR antenna to jam the front-door sensor. He then "spoofed" the unencrypted system by eavesdropping and recording a sensor radio-transmission message sent to the control panel and then retransmitted the same messages at a later time.

Lamb explained that he recorded a signal that indicated an alarm event was taking place then later sent that recorded signal to the system's control panel, which went into alarm because it had received an alarm signal — not from the sensor, but from Lamb's laptop. In effect, he could create false alarms on demand, which can result in many manners of havoc.

Keep in mind that spoofing is not jamming. Jam detection does nothing to prevent a hacker creating false alarms or remotely monitoring the movements of the alarm owner.

There is a Solution

Solutions to jamming and eavesdropping on radio messages have been around for a long time and already exist in some alarm systems. Jamming can be eliminated by using spread-spectrum technology (S-ST), which was developed by the military to prevent their radios from being jammed on the battlefield. The first radios were easy to jam once the enemy discovered the frequency/channel; after finding the frequency, all that was necessary was to broadcast a powerful "noise" signal on the same channel to blot out the message.

Spread spectrum prevents jamming because the message hops around on many different frequencies/channels to dodge the interference. An easy way to understand this is to imagine driving a one-lane road. All someone needs to do to jam traffic is to put a large van on the road in front of you. In contrast, spread spectrum is like driving on a 25-lane highway. If that same van attempts to block one lane, you simply change lanes to pass.

Like the driver on the 25-lane expressway, a device with spread-spectrum technology sends a message capable of switching channels to avoid traffic and interference. Although there are many variations of spread spectrum and methods of how the message chooses different lanes, the concept is the same.

Lamb also explained that encryption may be a successful tool to stop these attacks. For encryption to be effective in an alarm system, a sensor is programmed with a mathematical equation and a hidden numerical "key." To protect the integrity of the "key," it is never sent across the network, thus it cannot be intercepted. For every communication, the sensor sends a scrambled message to the control panel, which then reverses the complex equation to verify the identity of the sensor/sender and puts the message back in order. Each sensor also has a calculator that generates a one-time scrambled message for each radio transmission to the panel to further complicate things for hackers.

Suppose a hacker uses an SDR to eavesdrop on encrypted wireless communications and send a message from the door contact to the panel. When the hacker attempts to rebroadcast the recorded message, the panel knows to ignore the message because the one-time scrambled message has already been used and the time stamp is invalid. This is the same technology used to secure the data and the networks of the world's IP infrastructure.

While there are many types and levels of encryption, the Advanced Encryption Standard (AES) is probably most widely used. AES encryption protects both military and enterprise networks from hackers and eavesdropping. Keep in mind that nearly all encryption can be broken with enough time and computer horsepower, but this is the realm of the National Security Agency and beyond the reach of this level of alarm-system hacker.

The Message to Dealers

There are two options for security dealers: passively deny responsibility and accept the liability or proactively take action. Doing nothing equals losing the customer and the future contract renewals on which you are banking; being proactive and replacing the equipment or deploying mitigation technologies will allow you to remediate the situation and retain your customers far into the future.

To protect their customers, their reputation and the value of their companies, here are three things alarm dealers need to understand and do:

1. Understand that the world has evolved and new inexpensive hacking tools with accompanying "educational websites" are being promoted online. Single-frequency radios that are not encrypted can and will be hacked, spoofed and jammed — creating false alarms, fines and much worse.

2. Stop investing in a vulnerable technology that decreases consumer confidence in what you sell, increases your liability and loses value every day. Alarm dealers should install only wireless systems that use spread-spectrum radios and encrypt all communications.

3. Develop a strategy to replace the vulnerable equipment with state-of-the-art equipment that will retain value for years to come and regain the value your contracts have lost. If you do not replace the vulnerable equipment, be assured that there are companies and lenders out there that will take advantage of this opportunity to gain market share by taking away yours.

You Can't Rely on 2G Networks or POTS Anymore

By the end of 2016, AT&T will sunset its 2G network and many other Telcos are following their lead. Similarly, the telecommunications giant wishes to transition to Internet Protocol (IP) networks and dismantle the Public Switched Telephone Network(PSTN) during the next decade.

With the telecom industry focused on developing new infrastructure, you can expect aging copper lines to degrade, as investment dollars are committed to cellular technology.

What does this mean? Alarm systems using 2G cellular are defunct and phone lines are going away.

What are Your Options?
We believe the best solution to consider is IP alarm communication.

Although technology advances daily, IP technology appears to be stable enough that current equipment will not be obsolete in just a few short years. Although the initial cost of an IP communicator can be steeper, dealers can explain to customers that IP devices may eliminate the need for phone lines and that they will save compared to current GSM costs. In other words, the cost will be recaptured over time.

The foremost reason to select IP communication is the ability to cost-effectively poll the system's availability in shorter intervals, some as few as 60 seconds. This gives subscribers peace of mind that their system is working and they are always protected.

In contrast, with POTS (plain old telephone service) or cellular technology, polling intervals are usually set at 24 hours, meaning that a system could be down that long before a trouble signal is generated.

Also, increasing the polling frequency can increase traffic charges by cellular service providers.

Something else to consider is that the industry's largest alarm companies are going to market with an offering of alarm, video and home-automation systems using an IP backbone.

Through nationwide TV ads, those companies are creating a market and demand for such services. Keep in mind that as EMERgency24 alarm dealers, you have the ability to offer many of the same services via an IP alarm system.

By selling customers on next-generation technology now, you can also increase your recurring monthly revenue for years to come.

Digital Dealer Forms Saved with Your Company Info

To help EMERgency24 alarm dealers become more efficient, all of the forms needed to manage subscriber accounts are available digitally and allow data to be typed into the file and saved, thus eliminating some time spent on data entry.

These forms, which should be downloaded to your local computer and saved as a master file, are editable .pdf files that have embedded "fields" that allow you to key in data, much of which will remain the same for your customer base. This includes your company information, as well as some selections that you may choose to standardize, such as the date and time of autotests.

Additionally, as some dealers use the same base package of equipment for a majority of their customers, a "template" can be saved for these types of installations. Not only does this minimize data-entry time, but it enables you to provide a clean contract/form to present to customers.

Plus, the EMERgency24 Data Entry Department will be able to more accurately enter account information without having to decipher rushed handwriting samples.

Each of the editable forms is located in the password-protected Dealer Secure site under the Help/Literature tab.

Follow Laws (& Good Ethics) for Door-to-Door Sales

Door-to-door marketing is used by one of the fastest growing companies in our sector and EMERgency24 encourages dealers who go to market in this manner do so within the confines of the law. That means being familiar with local regulations, such as allowable hours of door-to-door sales and which communities require peddlers' permits. It is suggested that companies provide staff with identification cards that include a recent photograph, the person's name, physical description (height, eye/hair color) and clearly shows company name and license information.

By doing this, there can be no confusion about who your team represents, which is the biggest complaint by the industry about this sales method.

Continued from Page 1: Understanding EMERgency24 Account Numbers

card. These numbers can be found on the EM24 Dealer site, under your "Reserved Accounts."

4. If the panel allows more than four digits for the account, reference the installation manual to determine if the programmed account requires leading or trailing "fillers" or zeros (0).

Remember that our monitors are always willing to assist and can verify the line card phone numbers for your particular account.

EMERgency 24, Inc.
999 E. Touhy, Suite 500, Des Plaines, IL 60018
Ph.: 800.800.3624/info@emergency24.com

EMERgency24

EM24 Pays You to Install Videofied Hardware that Sends *Encrypted Signals* & Uses *Spread Spectrum*

Alarm dealers can optimize their cash flow and use their money as needed most

Video is the future of the industry and the provided equipment from EMERgency24 delivers a higher level of protection for subscribers.

- You pay nothing for equipment use.
  - We PAY YOU for installation.
  - We PAY YOU for new service agreements.
  - We PAY YOU for each renewal.
- Paid service visits after first year of agreement.
- Free training for sales people and technicians.
- Free leads from www.VideoMonitoring.com.
- Free mobile-compatible web portals for dealers and subscribers.

For more information on EM24 Video Monitoring, contact the Sales Department at 855.760.0030.

IDC 601 Door & Window Contacts

MotionViewer

XMA 621 Keypad

XT-IP 620 Control Panel