LASERSHIELD ALARM SYSTEM: A DETAILED ANALYSIS

The LaserShield Master Alarm Unit is the heart of the wireless "plug and go" alarm system.

Interview Tony Dohrmann, CEO of LaserShield
http://video.security.org/lasershield.wmv

Bypass of the LaserShield system within a residence
http://video.security.org/lasershield_bypass.wmv

Demonstration of the LaserShield system and bypass
http://video.security.org/lasershield_full_report.wmv

Detailed Technical Specifications Summary
http://download.security.org/lasershield_techspecs.pdf

This report details the results of our analysis of the LaserShield alarm system. We concentrated on issues relating to design, technical, operational, security, and suitability of the system for use in residential and commercial environments. A comprehensive list of issues was developed and which formed the basis of our product testing. Anyone considering the purchase of a home alarm needs to understand the security issues inherent in such systems. Although the price of the LaserShield is minimal (at about two hundred dollars for the basic unit) the real issue is an assessment of the convenience and security that is provided by this product.

As a consumer you rely on your alarm system to protect against physical intrusion into a home, apartment, dorm room or other area. If the electronic monitoring system does not afford adequate protection then it may be dangerous because it can create the illusion of security that may not exist. The purpose of any alarm system is to offer early warning of the presence of intruders and to alert the homeowner as well as the police. If you are considering the purchase of an alarm system or have already installed a LaserShield I would encourage you to read this report in its entirety. Although it is admittedly quite long it will also provide you with a better understanding of the capabilities and limitations of the LaserShield system so that you can make a more informed judgment of its suitability for your needs and whether it is secure enough to protect you.

Introduction

LaserShield is the first company that has designed a consumer-grade self-installed alarm system to protect residences and small businesses. Headquartered in Las Cruces, New Mexico, they have been touting the security that is provided by their unique "plug and go" integrated burglar and panic monitoring and reporting system.

When I first heard their claims in radio advertisements I was skeptical because an electronic alarm system has to be engineered properly and must rely upon a number of interrelated components and systems. Any design deficiency can place the security of the entire system and those who rely upon it in jeopardy. This is especially true in the case of a consumer alarm system because professional installers are not responsible for supervising the placement of trips, control panel, interface with telephone circuits, programming, and the selection of communication protocols with an approved central alarm reporting center. As a general rule consumer-grade alarms may be poorly engineered and do not have the R&D that is required to offer reliable protection.

Why was I so interested in this product? The short answer is that most residences rely on mechanical locks for their primary protection. In many instances this is just not enough security as I have noted in many previous articles. We call it "defense in depth" which means that other security measures to back up the locks, doors, windows and other physical barriers are implemented so there is no single point of failure. If a manufacturer markets a product that does not live up to its claims, especially a burglar and panic alarm system, then serious consequences can result because the user can be at risk to their life and property.

We conducted an extensive evaluation of the LaserShield system. We also asked a major U.S. alarm equipment manufacturer if they would do the same in order to confirm our findings. They did, and concurred in our results. I then traveled to Las Cruces, New Mexico to interview the CEO, Tony Dohrmann and his team of engineers and technical support managers. I also spoke at length with Clint O'Connor, Chief Project Engineer about the design philosophy of the LaserShield system and technical issues of concern.

Las Cruces, for those of you who are not familiar with Southwestern United States geography, is located about forty miles from the Mexican border. It is not at the end of the world but you can surely see it from there!

What we found in our research about LaserShield may surprise you.

Alarm Systems: A Technical Overview

There are three basic levels of alarm systems, depending upon the requisite security that is needed at a given facility. Exactly how much security will determine the sophistication of the installation, the type of intrusion sensors that are employed and their supervision (continuous monitoring), and the type of communications and remote monitoring that the system offers.

Commercial and government facilities usually employ hardwired sensors (called trips) to determine if a defined event occurs. These occurrences might include an intrusion beyond a defined perimeter, motion detection within a protected area, tampering, vibration or shock to objects (such as safes and vaults) temperature extremes, water flow, fire and other conditions. Most alarm systems are installed by a recognized and certified alarm company that is licensed to provide these services. Almost all jurisdictions have some form of licensing laws because of the dangers from improper or erratic operation, especially given the fact that the national average of false alarms is higher than ninety percent. Interestingly, most false alarms are generated by the user by improper set-up or disarming of their system. This is a problem that LaserShield has virtually eliminated by the use of a key fob rather than a conventional keypad for arming and disarming.

These alarm systems usually report to a **central station** facility either by dedicated telephone line connection or by dial-up, meaning that the control panel dials a specific number for the alarm center and transmits a series of codes to a remote alarm receiver. Some central stations are certified by Underwriters Laboratories to meet certain minimum security criteria because they are utilized for monitoring high security facilities. These systems are generally expensive to install and monitor.

Business and residential customers may also install alarms that utilize less sophisticated trips and fewer of them. These systems are usually much less expensive than a commercial installation ($300-$5000) and often use dial-up communications as the primary means to send information to an alarm dispatch facility. They are professionally installed but do not offer the same level of security.

In the third type of system, **residential customers and small business** owners may opt to install their own hardware. There are many different configurations that are available but generally they utilize wireless technology for communications within the home or business. Door trips and motion sensors **do not** have to be wired to a control panel (which is often expensive and a major hassle). All signaling between the individual trips and the alarm panel is done via radio and usually supervised on a one-way basis. This means that a trip fault is reported on a timed interval, often about every hour, rather than immediately.

Although these systems are inexpensive and relatively easy to install they are also not as secure as the more sophisticated installations described above. LaserShield falls within this third category.

There are many companies that offer wireless-based systems including GE, Honeywell (Ademco), X10, ITI, Linear Sentrol, Skylink, ITI and several other brands, so if you have one of their systems installed you are potentially at risk of the same bypass technique that we demonstrate in this report with regard to LaserShield.

The LaserShield System

LaserShield in my view is the first practical consumer level alarm system that provides a sufficient measure of security for residential applications. **It should not be utilized in a commercial environment** where any significant level of security is required because for all of its innovative features it also has serious security vulnerabilities that can be easily exploited by knowledgeable criminals. When I discussed this issue with the company, representatives of LaserShield made it clear to me that they were not concerned about "knowledgeable or determined" criminals but rather opportunistic or casual burglars.

The system is comprised of two primary components: the Master Alarm Unit (MAU) and wireless motion sensors. In addition, the company now supplies a communications module for use with VoIp circuits (called Sparrow) because of the problems with touch tone signaling over Internet telephony. For installations that require redundancy in communication links or for remote locations that are not supported by either telephone or Internet the manufacturer also produces a cellular modem for an additional monthly fee, called a **Cyclone**. This option only works on the GSM mobile network such as Cingular and T-Mobile so if these carriers do not have coverage in your area, this option will not work.

The **M**aster **A**larm **U**nit (MAU) contains the microprocessor-controlled logic, receiver and communications interface to allow monitoring of trips and to report an intrusion. The MAU is capable of addressing a total of sixteen devices that can include a combination of infrared motion sensors and wireless key fobs to turn the system on and off.

Presently the LaserShield system is based completely on wireless technology with regard to internal communications within the protected facility. The MAU is turned on and off by a wireless access device similar to the keyless entry unit that is used for cars. Unfortunately, as I will discuss subsequently, it is not particularly secure but is very convenient and user-friendly and will eliminate most false alarms. All of the motion sensors also communicate with the MAU via a wireless link so there is absolutely no wiring required. That is a real advantage because it is often impractical or impossible to run wires for an alarm system, especially in rental units.

The LaserShield system can be installed and ready to go in about five minutes, but there is a price to be paid for this convenience in terms of security. I will address this issue later in this report.

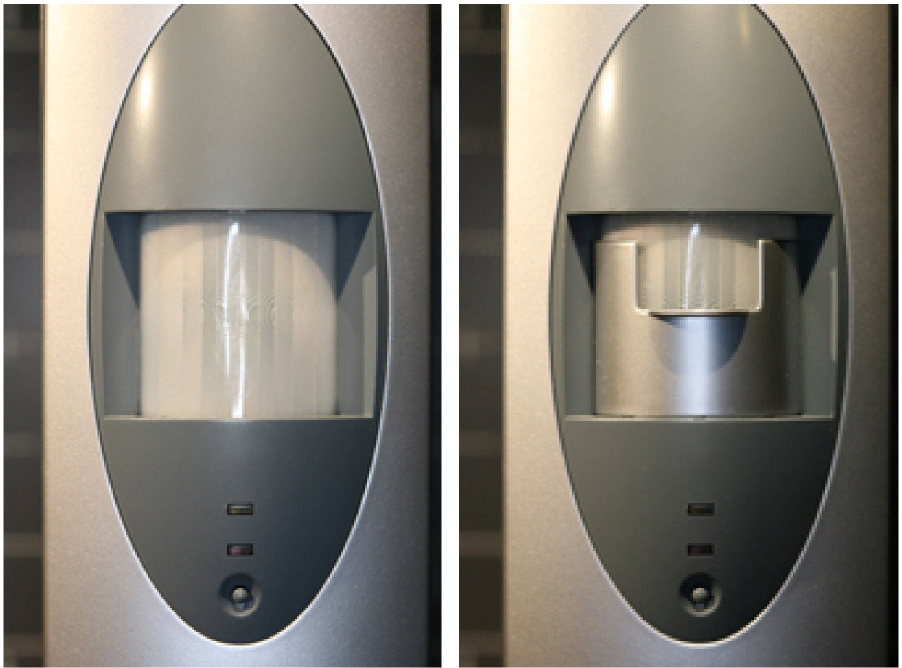
Comparison of LaserShield with other Alarm systems: An Overview

All alarm systems have essentially the same primary components and functions. We noted that differences in the sophistication and security of systems will depend on the number and types of trips, their grade (government, commercial or consumer) their internal supervision, the capability to process multiple trips by the central processor, and the mode of communications with the outside world.

Motion Sensors (Trips)

A LaserShield Passive Infrared motion sensor is inconspicuously placed in a bookcase.

The heart of every alarm system rests with its sensors or trips. There are many different types of devices for the detection of a wide range of events. Infrared, microwave, audio, electrical continuity, vibration, glass-break signatures, pressure sensitive materials, air pressure, photoelectric beams and many other technologies are available if they can be interfaced and analyzed by the central alarm panel.



The LaserShield motion sensor can be masked so it is insensitive to pets. The unit on the right has a plastic insert that covers most of the sensing area of the detector so it will not trip from small animal movement.

LaserShield presently has only one wireless infrared motion detection sensor available. This means that the user is limited to one form of protection. While this may be quite sufficient for most consumer-level applications it does not allow for any system flexibility. Tony Dohrmann (CEO of LaserShield) told me this is expected to change in 2008 and that the company will likely be expanding its line of trips to include fire, door contact and perhaps other devices that can be connected directly into the system. They will also provide a separate loud siren that can be installed to scare away intruders. Presently, only the noisemaker within the MAU is available.

Just how loud is the internal sounder? It was loud enough that a burglar who broke into a LaserShield protected home urgently attempted to silence the Master Alarm Unit by submerging it in a bathtub that he tried to fill with water. Ultimately, the house flooded because he left the water running as he fled!

Communications of an Alarm to a Central Station Facility

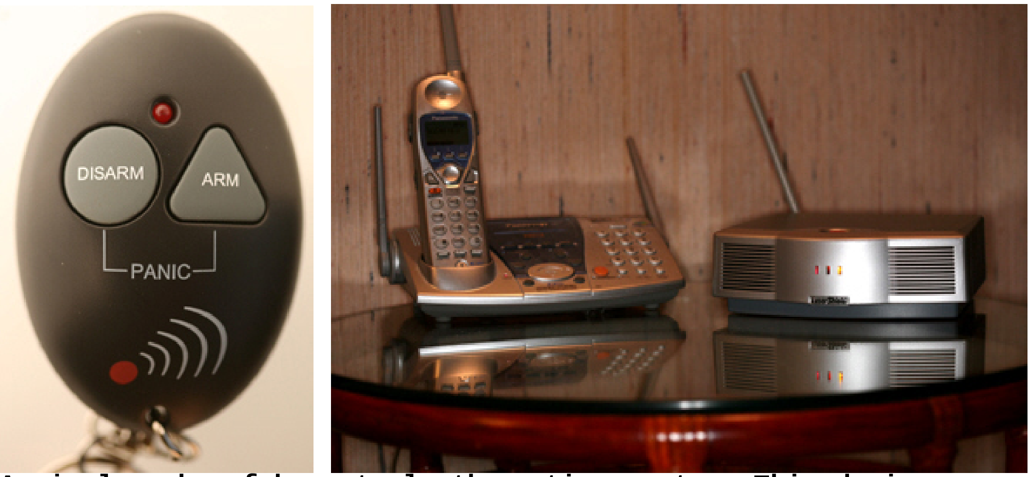
Properly engineered alarm systems must have the ability to communicate with a central dispatch facility for remote reporting. Some alarm panels may intentionally not be connected to a monitoring facility and LaserShield is no exception. The homeowner may rely only on the internal sounder. In some cases this may be sufficient to scare away an intruder because they do not know whether the police have been notified of the break-in.

Cost for remote monitoring may also be an issue. Presently LaserShield charges about $20 per month for monitoring services (and another ten dollars if cellular is utilized). This may be too expensive for some, especially students and others on low or fixed income. Although the LaserShield system will allow local reporting only I recommend that it be connected to a central station so a burglary may be reported to the police.

The LaserShield MAU is normally connected to a standard phone line. When it is armed and a trip is detected the unit allows for a slight entry delay and then will send an alarm if not disarmed. When the unit reports an intrusion it takes the phone line off-hook, dials a preprogrammed primary or alternate toll-free number for the alarm center and sends a series of high speed touch tone pulses to indicate the user ID number and trip identification for areas that have been penetrated. The data base at the alarm center automatically correlates the transmitted information and can notify the police as to the type of trip that is reporting. The Rapid Response monitoring center that LaserShield uses may have one of the fastest response times in the industry because the verification and reporting of all alarms is automated. This minimizes human interaction and can cut valuable seconds in police dispatch.

You should understand there are security issues with regard to any system that uses dial-up communications. Often there is unrestricted access to the connection panels that are used by the telephone company as a junction point to bring a circuit to the subscriber residence. If these lines are cut or disconnected then any dial-up system can be taken out of service unless it has backup communications.[1]

How the LaserShield System Works



A wireless key fob controls the entire system. This device has a fixed code that can be cloned with the proper equipment and expertise[2]. Normally the master alarm unit is located in a convenient location so the internal panic button can be activated in an emergency.

When you receive your LaserShield it consists of a Master Alarm Unit (MAU) and one or more motion sensors. It also typically has two wireless key fobs for control of the system. A detailed instruction booklet is also provided.

The LaserShield system is relatively easy to install and is quite straightforward. **Installation** involves the following steps:

The MAU is placed somewhere that is convenient to the homeowner and can also be heard by an intruder if the sounder is activated. There is a red button on the MAU and every motion sensor for panic alert.

The central unit must be plugged into commercial power but has a backup battery that will allow it to operate for several hours in the event of power failure. The design of the Master Alarm Unit backup battery is such that it is time-consuming to remove so as to deter a thief from disabling the system by disconnecting all power.

The motion sensors must be located according to the instructions in the manual and connected to power. They are usually placed about four feet above the ground and pointed in the direction of the area to be protected, which may extend to sixty foot coverage area. There are certain precautions that must be taken when utilizing IR in order to avoid false alarms. Infrared responds to changes in temperature so care must be exercised that the devices are not pointed at surfaces that rapidly change temperature such as windows and heat registers.

The MAU is connected to a phone line in order to communicate with an alarm center. A cable is provided with modular RJ11 connectors to allow the unit to be plugged directly into a wall jack that provides a telephone circuit. Although telephone connection is straightforward there are security issues with this method of interconnection that are not normally encountered in the more secure systems. Again, convenience must be balanced against security; most consumers do not know how to interconnect an alarm panel to a phone line other than by plugging a modular jack into the wall. Again, LaserShield made it as simple as possible.

If you subscribe to remote alarm monitoring with the Rapid Response central station then you must send an executed agreement to the company which is a contract for service. LaserShield has made the registration process quite simple, allowing for the customer to fax, mail, register on line, or sign-up at certain retail locations. Service can be initiated with little difficulty. Rapid Response is a DoD certified national monitoring center with an excellent reputation. LaserShield selected a reliable vendor to monitor their customer accounts and enhanced their capability with automated alarm processing.

Once the system is installed and connected and a test has been run with the monitoring center LaserShield will protect your residence when you press the "ARM" button on the key fob. You will have about a minute to leave the premises before the system is active.

To enter, simply press the "DISARM" button and the system is disabled. Verbal prompts will confirm arming and also indicate whether certain fault conditions exist that may impede proper operation.

Remote Telephone Access and Audio Monitoring

The LaserShield provides a limited form of remote and monitoring by allowing you to dial the MAU from a phone at another location. You can call the MAU from your cellular and monitor the audio within your residence for up to twenty seconds, press one of the touch tone keys to refresh the timer and listen for another twenty seconds. The system will allow continuous monitoring so long as the timer is refreshed every twenty seconds. I do have some security concerns with this scheme because of the potential ability to remotely monitor audio within a premise without the knowledge of the homeowner[3]. A password is required to access the system but if the password is compromised then the LaserShield could be used as a remote microphone.

System limitations

In my view there are three major system issues that may impact on the overall usefulness and security of the LaserShield concept. First and foremost is the limitation as to the availability of trips for monitoring intrusion and other conditions. This is probably the most serious drawback to the system but again, it is a low-priced solution to afford some form of protection to a specific class of user and may actually be sufficient to satisfy their needs. Not everyone can afford or is allowed to install more sophisticated alarm systems and so LaserShield clearly understands this niche market and has attempted to meet its specific needs with a very simplistic and well thought out approach.

Second, the manufacturer chose to make its system totally wireless within a protected facility. Consistent with their design philosophy that is probably their wisest (and only) choice but it presents a serious vulnerability that is shared with other competing systems that also rely solely upon wireless trips and control.

If you are willing to accept the possibility that anyone with a couple hundred dollars and knowledge that you are relying upon a LaserShield system can easily and instantly defeat your alarm then LaserShield will likely provide quite adequate monitoring and reporting of any intrusion into protected space. It comes down to a question of risk versus convenience and price.

If it likely that a burglar would go to the trouble of defeating your system then it may be of concern. But remember that the same burglar can also disconnect your phone line if the interconnection point is exposed, which would mean that no alarm would note be reported to the Rapid Response center in either scenario. The problem is that if your Master Alarm Unit is defeated by radio jamming then it will not send a report or make any noise to alert neighbors.

Third, because the LaserShield Master Alarm Unit is totally portable it can also be instantly unhooked from power and phone line by an intruder and disabled. To be fair, the unit has an internal battery that would allow it to continue making noise even if it is disconnected from mains power. If the unit sends a report to the monitoring center before the burglar can get to the MAU then it does not matter because the data has already been transmitted to Rapid Response.

If a jamming transmitter is employed then a burglar may not only break into your house or apartment but may also steal your LaserShield unit! You must consider whether the burglar that may target your house would try to bypass your alarm system by using a transmitter. LaserShield carefully considered the problem of jamming and decided the convenience and reliability of its fully wireless approach far outweighed the risk of radio interference which could disable the entire system.

There is no capability of programming the Master Alarm Unit to dial any telephone number other than is preprogrammed into the system to call the remote monitoring center. A very neat option would be to allow homeowners to set the MAU to dial their cell phones or other location to notify of an alarm, especially if the user opts not to use remote monitoring services. The company is considering this option in future product releases.

Analysis of the hardware

We conducted a detailed analysis of the hardware within the LaserShield system and were quite surprised at what we discovered. We also asked one of the largest alarm hardware manufacturers in the United States to examine the LaserShield in their laboratory. They did and concurred in our conclusions. See the link at the top of this report.

Detailed Analysis of Technical Security Issues

The following discussion presents an analysis of potential security vulnerabilities of the LaserShield system.

Wireless Communications between the MAU and Sensors

An inexpensive Motorola two-way radio will completely defeat the LaserShield and many other consumer-level wireless-based systems. We purchased our walkie-talkie through a dealer on the Internet for $300.

In my view the most significant threat to security is based upon the design of the LaserShield system and its implementation of completely wireless technology. The manufacturer chose this design mode to facilitate simple installation by the consumer. Unfortunately, simplicity never allows for real security and this is certainly the case for this system. Their primary design philosophy allows rapid bypass by a knowledgeable criminal.

Because LaserShield uses narrow-band RF technology it is possible for it to be easily jammed. There is no indication on the console of jamming and no provision to report the condition to the central station. When we ran tests with our jamming transmitter the system was rendered inoperative when the walkie-talkie was within 250 feet of the MAU.

It should be noted that most residential RF-based alarm systems can be jammed if the operating frequency is known. Some of those products that incorporate the more sophisticated and expensive spread spectrum or frequency hopping technology cannot be circumvented in this manner, but this is not true for every product[4]. The LaserShield operating frequency can be easily found in the FCC data base because the company filed for a Part 15 registration.

So how easy is it to defeat the LaserShield system? It is trivial so long as the intruder has access to an inexpensive radio transmitter that is programmed to the correct UHF frequency. These radios can be ordered from Motorola or a simple transmitter can be constructed. In our test we utilized a Motorola walkie-talkie that was programmed to the LaserShield frequency. To completely defeat the system all that was required was to continuously key the transmitter prior to entering a protected zone and make certain that the transmitter remained on until we left the premises. That is it! See the video of the author entering a townhouse and how easy it was to bypass the system.

Because of the excellent characteristics and extreme sensitivity of the LaserShield receiver the useable range of our transmitter was no problem from outside of the protected residence. The entire system is based upon radio communications and because the motion sensors are not continuously monitored (as with traditional hard-wired trips) the system has no way of knowing if a trip sends an alarm if at the same time the receiver is made inoperative.

Keying a transmitter blocks the receiver from "listening" to any of the sensors and so it never knows whether an intrusion has occurred. This is precisely the problem with systems based totally on wireless trips, especially at the consumer level. For this reason we believe LaserShield should never be deployed for commercial applications. It would be my advice NOT to place any LaserShield alarm stickers on the outside of a protected premise because it is an advertisement that the system can be easily defeated.

Summary of Security issues

It is recommended that LaserShield window stickers not be displayed because they are advertisements to knowledgeable burglars about the type of system that is installed.

There are several security concerns that should be considered by the consumer. These issues can, in the view of the author, enable system bypass, limit the ability of the homeowner to fully utilize the system, and result in reduced protection.

The product’s make-up is such that detection only occurs after the burglar has entered the premises. This is considered to be a drawback because optimally the system should act as a deterrent and discourage entry into the protected premises. No perimeter trips or other sensors can be connected to the MAU at this time. In fairness, systems with perimeter protection typically cost much more than LaserShield.

The basic kit will cover only one or two rooms. Other rooms will require additional detection devices to provide adequate coverage throughout a residence. It should be noted that many competitive systems also require added devices (at additional cost) in order to provide adequate protection.

Summary of Product Advantages

- **Cost:** Inexpensive system (about $200 for entry level) that is suitable for the protection of residence locations, especially where it is not possible to install hard-wired trips;
- **Installation and Setup:** System setup with the Rapid Response monitoring center is very easy. Installation of the system is fast, simple and uncomplicated. No technical ability is required;
- **False Alarms:** The systems drastically reduces the primary cause of false alarms: keypad entry error. By using a simple key fob with two buttons (arm and disarm) they have made it fool-proof for the consumer;
- **User interface:** The voice prompts are clear and easy to understand and are now available in Spanish as well as English. The status of the Master Alarm Unit and any fault conditions are provided by explicit voice prompts;
- **Range and placement of trips:** Excellent receiver sensitivity for long range operation of the motion sensors;
- **Bypass of sensors:** Motion sensors can be easily bypassed by the user for night activation;
- **Siren:** The internal siren is protected from damage and would be difficult for an intruder to disable in a short period of time;
- **Technical and Operating Information:** The instruction manual is clear and fairly concise, although it could provide more detail. It contains sufficient information for us to install, test and monitor the system;
- **Motion sensor performance:** Good PIR sensitivity and transmission range. The sensors should reliably work within almost any residence;
- **Response time:** The Rapid Response Center provides an automated system to reduce the time from when an alarm is received until notification of police;
- **Adding trips to the system:** Adding sensors is straightforward and easy and has set the standard in the alarm industry for user interface. Voice prompts indicate that each device has been learned by the system and the status of both the trips and MAU;
- **Quality:** The system utilizes high quality electronics and state-of-the-art technology;

- **Transmission protocol:** Contact ID is employed as a reporting format for the Master Alarm Unit to the central alarm center. This is the most accepted communications protocol in the industry.

Summary of Product Advantages or Negatives (Depending upon your perspective)

- **Backup battery:** The Master Alarm Unit will power-up if there is no AC power connected. This means that the backup battery could go dead within a few hours if mains power is not restored. In case of power failure this may be a valuable options but could also place the homeowner at risk of an MAU failure;

- **Bypass of trips:** The user must bypass devices at night to allow movement within a home or other facility. In the more expensive systems trips can be bypassed from the master keypad. Some users feel that the ability to easily take individual motion sensors out of service is an advantage, especially at night. The MAU will report that a trip has been bypassed upon arming. The problem is that someone who has access to your alarm can disabled trips and you may not know it;

- **Battery status:** There is no method to determine the status of backup batteries of the Master Alarm Unit if it is plugged into mains power. The unit will only report the status of its internal battery if it is not connected to power. LaserShield has an automatic battery replacement policy for all customers that subscribe to monitoring service. A new battery will be shipped every four years which will insure that the internal backup is always functional. The backup battery within each **motion sensor** will verbally report its condition to the user through the MAU;

- **Re-Programming of the MAU:** The MAU has no ability to be programmed for different reporting numbers, communications protocol, or entry and exit delays. Unlike other alarm panels the LaserShield can never be used with another monitoring service. The unit is preprogrammed for all parameters which apparently most consumers prefer. These issues may not be relevant for the LaserShield users because of their desire for an alarm solution that requires no significant interaction or expertise. Essentially the system offers only those options that LaserShield determined were the most desired by their target market. The user is locked into LaserShield if they wish to continue using their system;

- **Remote audio monitoring:** If the Master Alarm Unit is dialed from a remote location the caller can continuously monitor the audio that is picked up by the internal microphone. There is no warning tone or other indication that remote monitoring is occurring. This feature could be used by parents, for example, to check on their children if they are being taken care of by a babysitter. Although a password is required to access the MAU it does present the potential for unauthorized audio intercept and eavesdropping within a protected residence. The system will time out in twenty seconds if the caller does not refresh the system by pressing a key on the keypad.
- **Armed without being connected to a phone line:** The MAU can be unplugged from the phone line and disabled. It will verbally advise the user of this condition but if the user does not understand what this means it can be overridden and armed. In such event the MAU would have no way to report an alarm. This is also a positive feature for those users who choose not to subscribe to monitoring services.

- **Portability of LaserShield:** The Master Alarm Unit can be easily disconnected from phone and power and removed from the premise unlike professional alarm panels that are mounted to walls and may be difficult to locate during an intrusion. The LaserShield announces its location by making noise, although if it is connected to a phone line it may send a report before it can be disconnected. Portability can be viewed as either a positive or negative option. It is positive for the homeowner who wishes to move and transport the system to a new location. It is a negative from the aspect of security;

Summary of Product Negatives and Perceived Design Deficiencies

We perceive the following design deficiencies with regard to the security of the LaserShield system:

- **Wireless only:** Inability to control the unit other than by wireless;
- **Defeating the system with the phone line off-hook:** Connection of the LaserShield to a modular telephone jack means that the phone line can be interrupted by taking another phone off hook within the premises or outside where phone lines are terminated. Normal hard-wired panels actually interrupt the phone line so this specific condition cannot occur;
- **Cloning the key fob and intercepting information from trips:** Failure to employ a more secure system to identify the key fob. Each wireless device has a unique electronic serial number that could result in the ability to intercept, clone and reproduce a devices. The code of the key fob could theoretically be cloned by monitoring because rolling codes are not employed. A knowledgeable intruder can monitor the user while they arm and disarm the system and capture the identification code of the particular key fob and then reproduce it. Information that a LaserShield system is in use can theoretically be obtained by monitoring the transmission that is sent from each trip to the MAU but this would be more complicated[5]. Users should never give their key fob to strangers such as valet parking attendants because of the potential to read and clone the electronic serial number of the device;

- **Pet masking:** Ability to circumvent the **P**assive **I**nfra**r**ed sensor if it is masked for pets. It is possible for an intruder to crawl below the field of view of a motion sensor that has been set to protect against false trips from pets. A PIR that is masked for pet immunity will allow an avenue for the burglar to gain access without tripping the alarm. Note that it is doubtful that a burglar would have this information prior to breaking into the protected premises but it is a potential security vulnerability, especially if the premise is "cased" prior to entry. The design of the motion sensor is such that they are easy to identify as to their purpose, location and area of coverage;
- **Anti-Masking PIR:** Ability to block PIR devices by masking, which effectively takes them out of service. A motion sensor can be easily made inoperable by inserting a piece of cardboard or other material in

front of it or simply by turning it toward a wall or other solid object. This could be a problem if a service person who had access to the residence was aware of the insecurity of these particular trips and their vulnerability to masking. In such a case the trip could be taken out of service without the knowledge of the homeowner. Commercial motion sensors integrate anti-masking circuits to prevent this technique from being employed;

- **Status Report on Motion sensors:** There are no status report on blocked motion sensors. The system will not know if a PIR has fallen on the floor or been masked with a piece of cardboard or other material;
- **Form factor of motion sensors:** Poor form-factor of the PIR devices which can allow them to easily be moved, turned toward a blocking surface, or fall to the floor. If a child or animal were to knock a trip to the floor the system could be armed without knowing that a motion sensor was not operating properly. The detectors are too large and cannot be mounted or affixed to any surface;
- **Internal siren only:** Failure of the Master Alarm Unit to allow connection to a remote siren to scare off intruders;
- **Surge protection:** No surge protection for power or phone lines which means the unit may be damaged in a lightning storm;
- **Radio jamming:** Sensitivity of the receiver to a jamming transmitter is high;
- **No programmable options:** Operating parameters are limited to **home** or **away** and cannot be altered;
- **Remote detection of the presence of a LaserShield:** It may be possible to detect if a LaserShield is in use by remotely sensing radio emissions from the MAU unit, from trips reporting to the MAU, or from the use of the key fob for arming and disarming. LaserShield is not the only alarm system that utilizes its specific UHF frequency so the burglar would have to be able to determine where the radio transmission had originated. By using the proper equipment and expertise it would be possible to determine that a LaserShield was in use at a particular residence. This information could then be used to jam the MAU receiver to completely bypass the system with an inexpensive two-way radio, as demonstrated;

- **Disabling of motion sensors to defeat the system:** The motion sensors report to the Master Alarm Unit about once an hour but are not two-way supervised which means that the user may not know that they have been turned off. If the MAU is powered down, then a trip turned off, and the MAU turned back on the homeowner will not be aware that a sensor has been taken out of the system. This could potentially occur if someone who had access to the residence and was knowledgeable about the LaserShield system had set the system so it could be bypassed. However, each sensor has a red LED indicator which would also be off so the homeowner does have the ability to visually determine if a sensor is operating;
- **Motion sensors are the only available trips:** No perimeter protection is afforded other than by using the PIR sensors;
- **Remote status indicator to user:** There are no status lights or key fob remote data for the homeowner to learn the status of the system from outside of the residence;
- **Status reporting:** There is no daily/weekly/monthly check-in feature to the alarm center to verify proper operation;
- **Reporting of system radio jamming:** There is no way to report system jamming status to the central station or on the console. There is no RF threshold indication on the MAU unit to alert the user that there is interference that could result in erratic or unreliable operation;
- **Operating temperature:** This unit cannot be used in unheated areas where the operating temperature drops below forty degrees or where there is significant condensing humidity;
- **Silent alarm:** There is no silent alarm capability when the panic button is depressed;
- **Arming the system with no active trips:** The unit we tested could be armed even though there were registered but non-active trips in the system. This means that although a trip has been added to system memory it can be taken out of service and the Master Alarm Unit will not know it;
- **No Dual-technology motions sensors:** The motion sensors are not dual-technology, meaning that they are more prone to false alarms from a rapid rise in temperature. In the more sophisticated devices both

microwave and infrared sensing must occur simultaneously in order to validate an alarm;

- **No sensitivity adjustment or interchangeable lens on the motion sensor:** There is no sensitivity adjustment on the motion sensor in order to adapt its operation to a specific environment. There is no interchangeable lens and thus no provision to adjust the coverage area and sensitivity. Many commercial PIR devices supply different lenses to adjust the field of coverage;
- **Hardwire capability:** There is no provision for any hard-wired trip or on/off switch to be connected to the MAU module;

Technical Conclusions

LaserShield provides a simple-to-install means of providing basic intrusion detection within a residential environment. It is not designed to offer high-end protection and cannot be upgraded to offer advanced options. It is intended to provide protection in a do-it-yourself package. The installation can be performed by someone that has no security expertise whatsoever. The basic product is limited in its capabilities and includes one PIR, one Master Alarm Unit and two arm/disarm/panic pendants.

Installation was fast and simple. Adding sensors and key fobs was easy to accomplish and may be the most straightforward procedure in the industry. Voice prompts announce as each device is learned and the status of the master console. The instruction manual provided the information necessary to install, test, and monitor the system. The product works as advertised.

The quality of the devices are consistent with a retail security system; the electronics are sophisticated and well made. The console receiver incorporates state-of-the art technology as do the transmitter devices. RF range is acceptable and the alarm communicator incorporates the most widely accepted transmission format in the industry.

Conclusions and Recommendations

LaserShield has produced a user-friendly innovative and truly "plug and go" consumer-level alarm system that is a cost effective solution for home owners and renters. The system will provide sufficient protection for basic alarm services and can be easily transported to a new residence, unlike traditional hard-wired systems. LaserShield offers the ability to communicate via dial-up phone line, VoIP Internet circuit or by cellular so the system can be deployed virtually anywhere.

Many consumers do not have wired communications service but have opted to utilize cellular as their only phone. In such cases other alarm systems such as ADT and Brinks may not work because they normally require traditional dial-up circuits. LaserShield is ideally suited for these installations.

I would recommend the use of the LaserShield in consumer level residences, apartments, dormitories and other areas where a very simple intrusion detection system is all that is required. However, if more sophisticated protection is needed then LaserShield is not suitable and should not be considered.

[1] Dial-up alarm systems are inherently insecure because it is easy to disconnect telephone lines at the interconnection point to most residences.

[2] In theory the wireless key fob can be cloned because it utilizes a fixed electronic serial number and its frequency can be easily determined.

[3] In order to or remotely monitor audio, two things must occur: the phone number must be dialed twice within a few seconds and a password must be entered from the remote location. An eavesdropper could set the unit to monitor prior to the return of the residents if he had the password.

[4] Certain units that use spread spectrum or frequency hopping can be jammed by transmitting a carrier over the entire spectrum that is utilized or on the parking frequency for systems that employ frequency hopping.

[5] Based upon timing and range issues it might be impractical to intercept the needed data from individual trips. LaserShield has made this more difficult because other packets are transmitted that may have no relevance to an intruder and some encryption is also employed.