computers are bad

You are receiving this facsimile because you signed up for fax delivery of this newsletter. To stop delivery, contact Computers Are Bad by email or fax.

https://computer.rip - me@computer.rip - fax: +1 (505) 926-5492

2022-10-22 wireless burglary

Long time no see! The great thing about *Computers Are Bad* is that you get exactly what you pay for, and theres a reason Im not on Substack. Rest assured I am still alive, just very occupied with clients AWS problems and the pleasantly changing weather here in New Mexico.

Speaking of pleasantly changing weather, its the time of year when returning diurnal temperature swings start causing the shock sensors start to fall off my windows. I could provide a lengthy discourse on which adhesive products hold up to this abuse better (transparent 3M VHB seems like the best so far), but instead its a good opportunity to return to a topic that I introduced right about a year ago: burglar alarms.

While there is a lot to talk about with commercial burglar alarms and their history, I want to start out our more in-depth discussion with something practical: security analysis of the modern home alarm market, which consists mostly of consumerized systems like Amazon Ring (the burglar alarm company they acquired, not the doorbell), SimpliSafe, etc. Youve almost certainly seen or heard advertising for these products, and they have the major advantage of being surprisingly inexpensive. A complete Amazon Ring burglar alarm installation can sometimes cost less than just buying and mounting the cabinet for a conventional alarm system.

Just to be clear on the differentiation Im making here, a conventional alarm would be one made by a long-established company like DSC, Interlogix, or Honeywell. It can be a bit hard to trace due to a lot of M&A history, but these companies have been manufacturing burglar alarms for 50+ years. Most ADT alarms, for example, are rebranded Honeywell (often from the era when it was Ademco, later acquired by Honeywell). These systems are mostly the traditional architecture of a control cabinet and wired sensors and panels, although all of these manufacturers offer hybrid solutions with various types of wireless sensors. Perhaps most importantly, these systems are mostly the same as commercial alarm systems. Sometimes the same model is certified and sold for both home and commercial use, sometimes the home version is feature-limited, but they use the same basic concepts.

When I talk about consumerized systems, I am referring to Simplisafe, Ring, Abode, etc. This whole new generation of alarm systems are typically cheap, completely wireless, and sometimes even controller-free. Theyre catching on because of their low cost but, perhaps moreso because of the different sales model. Conventional alarm systems were distributed entirely through a dealer network. A home alarm system was typically installed, monitored, and maintained by a local dealer, who might even set a programming password... ostensibly to protect the consumer from compromising their

own alarm, but often in practice to complicate adoption of the alarm by a different dealer. Dealers usually made most of their money off of monitoring contracts and viewed the actual alarm as a loss leader, which is why you might remember television advertising for free alarms from ADT. ADTs dealer network will indeed install a very basic alarm system for free, but they will lock you into multiple years of monitoring at a relatively high rate. Classic razor-and-blades behavior.

More consumerized systems today, though, are usually sold direct to consumer with low-cost monitoring from their vendor (or in practice, a UL certified monitoring center contracted by their vendor). Monitoring is often contract-free and they usually have a pretty rich self-monitoring feature set based around a mobile app [1]. In general, they feel a lot more like a consumer tech product and a lot less like a home utility advertised mostly on the side of aged Econoline vans.

Like most consumer tech products, they are also heavily cost-engineered, emphasize the appearance of features over good design, and are sometimes downright poorly thought out. Obviously I am rather critical of this generation of products, but I should make it clear that the news is not all bad: *they are very cheap.* There is an important trade-off here between cost and performance, and a low-cost option isnt necessarily bad. To twist a common expression, the best burglar alarm is the one you have, and the high installation price of conventional systems has long been a deterrent.

Lets take a look at some of the design decisions of these consumerized alarm systems and how they relate to security properties.

Controller vs. Controllerless

The most prominent brands of consumerized alarm systems make use of a controller which is separate from the panel(s). However, there are several vendors that sell controllerless systems where the main panel also contains the controller. To be clear, when I say panel I am talking about the thing that you usually mount next to an exterior door and use to arm and disarm. The user interface of the alarm. The controller is traditionally a metal cabinet with some PCBs in it but for these consumerized systems often looks more like an outdated Apple AirPort, and goes... somewhere. Traditionally a bedroom closet, but you could put it just about anywhere, preferably out of sight.

A different but related issue is whether or not there is a siren built into the controller, or the siren is a separate device. UL certification requires a siren and so there will always be one somewhere, but many systems reduce cost and installation complexity by building it into the controller... something that is exceptionally rare with conventional systems.

The main consideration when comparing a system with a controller to one without a controller is smash-proofing. When a burglar violates the alarm by entering a secured house, they are typically free to roam for the duration of the entry delay period, which is usually 30-60 seconds [2]. Conventional alarm systems intentionally place the controller in an out-of-the-way location and preferably one protected by immediate zones (or at the minimum a key lock and tamper switch on the cabinet door), to avoid a burglar tampering with the controller during the entry delay period. The reason for this may be obvious: if the burglar can destroy the controller before the entry delay period ends, the alarm may never be reported. Of course if the controller is built into the panel next to the door this is very easy to do. Its also easy to do if the

siren is built into the controller, since it provides a convenient homing signal [3].

Of course there is a technical method to avoid this problem. If the alarm reports to the monitoring service that the entry delay period has started, the monitoring station can independently time the entry delay. If an alarm disarmed message is not received within the entry delay period, the monitoring station can assume that the controller was destroyed or communications prevented, and treat the situation as an alarm. Different vendors have different names for this concept, which range from smash-proof monitoring to asset protection logic (???). Older conventional home alarms usually didnt do this, because they had to intercept the phone line, dial a call, report the message, and release the phone line for every monitoring event. This took long enough that it was to be avoided, and so it was common to not even report disarm events. Newer conventional and consumerized alarms report mostly by IP, and packets are cheap, so theyre more likely to report every imaginable event.

One of the pain points here, though, is lack of clear communication. It can be hard to tell whether or not a given alarm system is smash-proof based on the marketing. As a matter of principle, I tend to mistrust controllerless designs since they are missing the first ring of the defense-in-depth tamper protection strategy (making it difficult to locate the controller). That said, a well-designed smash-proof monitoring strategy can mitigate this issue. It ultimately comes down to how much you trust the vendors monitoring implementation.

Reporting paths

Another consideration in the design of alarm systems is the reporting path. If a burglar can prevent the alarm reporting in, they can roam the house undetected until a neighbor or passersby hears the siren and calls the police. In practice people mostly ignore sirens, so this could take a very long time. Its very important that the reporting mechanism of the alarm be reliable.

Conventional alarm systems perform reporting using a communicator, typically a module installed in the cabinet. Communicators can be swapped out and there are many options available for most alarms, giving you a good degree of flexibility. Consumerized systems typically have one communication strategy built into the controller, but often enough its the good one anyway.

Older alarm systems reported by telephone, leading to the trope (and reasonably common practice) of burglars cutting the phone line before entering. Modern alarm systems are much more likely to report over the internet. The great thing is that this makes dual-path reporting much easier: most consumerized alarm systems have either a standard or optional cellular data modem that allows them to report either via your home internet service *or* via the cellular network.

Given how low-cost it has become, dual-path reporting ought to be the minimum standard today. Fortunately basically all alarm systems offer it, conventional and consumerized. Consumerized systems typically ship with a fully integrated cellular feature with service sold as part of a monitoring plan. Modern communicators for conventional alarms are often LTE Cat-1 based but, unfortunately, its not unusual for them to be locked down to a specific message broker.

Once pro of conventional communicators, though, is that all the major models are available in both AT&T and Verizon variants. This might be an important consideration

for homes with poor cellular service from one or the other network. With consumerized systems it can be hard to know what network they use, and I havent so far seen one with a solid site survey feature to establish that the cellular connection will be reliable. This is the kind of thing that feels like an artifact of the product having been designed and tested only in an urban area, where its safer to assume that any given cellular provider will be workable from inside a closet.

Wireless Everything

And here we reach the elephant in the room: wireless sensors. The largest cost in installing an alarm system is usually the labor to run wiring, and it often ends up being installed in visible ways to hold down this cost. Homeowners hate visible wiring and they hate the high labor cost of installing wiring in walls, which can be hard to do without leaving visible artifacts anyway.

A variety of different protocols are in use for wireless alarm systems. Conventional alarm systems introduced 433MHz sensors decades ago, and these are still in fairly common use. These sensors use a very simple PSK modulation to send typically around a dozen bits, including an address and some payload. There is no encryption or authentication. On the upside, the lack of any sort of cryptography makes it very easy to implement receivers for these sensors, and most conventional alarm radio modules can support 433MHz sensors from any manufacturer. This is viewed as an enduring feature of 433MHz sensors, since alarm dealers often perceive proprietary encrypted schemes as being mostly motivated by vendor lock-in.

So, about those proprietary protocols. The major alarm vendors have introduced various newer wireless protocols that are both more sophisticated (in terms of payload size, architecture, etc) and more secure (through use of cryptography). An example would be DSCs PowerG, which uses AES encryption, spread spectrum, and dynamic transmit power selection to deliver more reliable performance and resist jamming and replay attacks. PowerG is a far better design than traditional 433MHz, but of course you will have to buy all of your sensors from DSC... and they arent cheap.

Consumerized alarms are more likely to use an industry standard protocol, and some conventional alarms do as well, at least as a secondary feature aimed at home automation. Z-Wave is probably the most popular (Amazon Ring, for example), although Zigbee is also in play and we can probably expect 6LoWPAN on some upcoming product. While this might seem to eliminate lock-in, well, its typical for consumerized alarms to have a whitelist of approved sensors. Some of this is of course profit maximization, but there is also a real contradiction between open ecosystems and UL certification (which is typically required by insurers in order to offer a discount).

Use of open standards is not universal in these newer alarms. Abode, for example, uses a proprietary protocol in the 433MHz band for alarm sensors (although the controller also has Z-Wave connectivity for automation) [4]. All in all the whole thing is kind of a mess, and its not necessarily easy to determine what radio protocol a given system uses. This is especially true for conventional alarms where the radio interfaces are often multi-protocol and there may be a mix of different devices in use, either to reduce cost or due to expansion over time.

All of this talk of radio raises a very obvious question: are these alarm systems adequately resistant to malicious interference?

Well, its sort of hard to say. Jamming of WiFi-connected surveillance cameras has been observed in home robberies, so at least the more sophisticated thieves are clearly aware of the possibility. That said, I put jamming in scare quotes because as best I can tell the attack in question is actually deauth spamming. This is not proper radio jamming but rather exploits a weakness in the availability design of the WiFi protocol, and as a result its significantly more practical and devices to perform the attack can be purchased online.

Actual jamming tends to be more difficult because it requires higher transmit power than legally manufactured (and thus readily available) radio ICs are capable of, and spread-spectrum or frequency-hopping designs are inherently resistant to interference. While there are academic papers describing practical jammers for 802.15.4 based protocols like Z-Wave and Zigbee, I have not been able to find any evidence that these devices are in use by burglars or even possible to obtain or build without the electronics and software engineering knowledge to build one based on the research reports. That said, with the magic of international ecommerce there can sometimes be an extremely rapid tipping point from attack not practical to device available on AliExpress for $20 [5], so its important to stay abreast of the developments here.

It should be said, too, that classic 433 MHz devices are so prone to jamming that its not unusual for things like garage door openers to cause intermittent supervision troubles. Unfortunately these types of sensors really shouldnt be used, which is part of why major manufacturers dont really want to sell them. Plenty of alarm installers still go out of their way for the lower cost of these obsolete sensors, though, and like HID Classic far too many vulnerable examples can be found in the wild.

Manufacturers of wireless alarm systems sometimes contend that jamming is a non-issue because sensors are supervised, by sending regular pings to each sensor and confirming a response. Ignoring the obvious issue that most of these alarm systems seem to treat an unreachable sensor as a trouble rather than an alarm even in the armed state, supervision of wireless devices is truthfully only really designed to handle low batteries or hardware failure, not tampering. Consumerized alarm systems usually dont allow configuration of the supervision interval and dont even tell you what the supervision interval is. Conventional alarm systems often have a configurable supervision interval but its usually still quite long as a minimum. One hour, four hours, and even 24 hours are all fairly common supervision intervals for RF senors. In practice, a burglar would be able to jam radio contact with sensors for quite a while before even a trouble was raised.

So is this all an argument that wireless alarm systems are bad? Well, once again, the best alarm system is the one you have. That said, there is a distinct advantage to conventional wired zones, if nothing else in that it eliminates batteries as a trouble point. A big upside to conventional alarm systems is that they virtually always support wired zones alongside wireless ones, allowing you to hardwire where practical and use radio where it would just be too laborious.

Sensor Selection

One of the benefits of wired alarm zones is that their simplicity means that you have almost complete interoperability of all sensors (the exception here is those alarms that use addressable zones, but these are still quite uncommon for security systems). A dizzying array of different types of sensors are available from the conventional (magnetic door contacts) to the exotic (capacitative proximity sensors). Even for

proprietary wireless sensors, conventional alarm manufacturers offer a far wider range than the best consumerized systems.

For consumerized alarm systems, the selection of available sensors is often quite slim. This isnt necessarily an issue for home installations, but windows can be an issue. Windows are one of the easiest ways to break into a house, and yet some consumerized alarm vendors offer almost nothing to detect broken windows. Acoustic glass-break sensors are fairly widely available but somewhat notorious for false positives. Direct-contact impact sensors are one of the best options available for windows but arent available for most consumerized alarms, and for others are obscenely expensive (considering that you ideally need one for each pane of glass) due to the placement of a complete radio module in each unit.

The sensor selection for consumerized systems can honestly be somewhat limiting, compared that outdoor PIR sensors for roof coverage and IR fences for outdoor perimeter protection are reasonably common on commercial alarms (and required by insurers for some types of businesses). These sensors are hard to find in any consumerized system, but widely available otherwise. In the past Ive desoldered the reed switches from door closures to connect conventional alarm sensors to a proprietary wireless system. This works well but its a hassle and requires a certain level of skill and equipment.

Monitoring Stations

Whenever possible, burglar alarms should be monitored by a central station. Traditionally many alarm dealers operated their own small central station, and many cities still have one or two of these small independents. Many conventional alarm vendors and all consumerized alarm vendors, though, contract with large nationwide central stations.

There is a certain degree of commonality between central stations because they all work to comply with the same UL (and sometimes FM) certification requirements. That said, consumerized alarm systems seem to choose their central stations based strictly on the lowest bid, and in my experience it shows. There can be a very obvious disconnect between the contracted central station and the alarm vendor that results in confusing information mismatches, and some cheaper central stations seem to use a live operator only to the minimum extent they think will pass UL muster... with most of the phone calls made by text-to-speech, making it difficult to get clarification or cancel false alarms.

Many municipalities and counties also have permitting requirements for alarm systems due to the burden false alarms can pose on police and fire departments. Some consumerized alarm vendors seem good at helping their customers take care of permitting, while others are not. A local company will pretty much always help you through this process and make sure your permits stay current... an important consideration since many municipalities will deprioritize calls from non-permitted alarms and then charge a fine for false alarms on non-permitted systems.

To be clear, I am depicting central stations in the most positive possible light. Large alarm dealers like ADT became notorious for their 2005-cellular-carrier behaviors of locking customers into long contracts at high rates. One of the advantages of having a conventional system that you own outright, though, is the ability to pick and choose central stations and change when you arent happy.

Consumerized systems tend to offer cheaper pricing on monitoring to start, but you are locked in to monitoring through the vendor until you replace the system. This is unusual with conventional systems where competitive monitoring services are usually able to adopt existing alarms, even if it requires sending a technician to reset the programming password.

Video Verification

Perhaps the greatest innovation in burglar alarms in some time is video verification, in which a monitoring center dispatcher receives either a recorded video clip or live access to surveillance cameras during an alarm condition. Its thought that police departments will prioritize calls more highly when the monitoring center operator is able to confirm that there is an actual break-in. Unfortunately, while there are common standards for video verification established by the Security Industry Association (SIA), in practice its usually only workable when the burglar alarm and video surveillance were purchased from the same vendor. Since consumer video surveillance systems tend to be uniformly terrible, theres a lot of downside here. Still, if you are willing to stay entirely in one vendors cloud-based ecosystem, look for one that offers video verification.

Conclusions

This is sort of a grab-bag of thoughts on how conventional and consumer systems compare. Generally speaking, conventional alarm systems are superior on pretty much every measure except for installation cost, where even in fully-wireless applications they tend to run a lot more. Compare, for example, a basic Amazon Ring startup kit at $249 vs. a basic DSC PowerSeries startup kit at $580 from one vendor that sells direct-to-DIY.

As one mitigation to the higher cost of conventional systems, they routinely stay in service for a good decade or more, which seems unlikely for products like Ring. Conventional alarm communicators are mostly monitoring-station-agnostic, allowing you to shop around for a monitoring contract and potentially save quite a bit of money. As an added advantage, in most cities its possible to get a monitoring contract with a local company that is either also a private security firm or has a relationship with one, resulting in a private security response thats typically quite a bit faster than police. You can usually make this kind of arrangement with consumerized systems by including a local private security dispatch as a contact phone number, but the contract monitoring centers arent really set up for it and you lose the benefit of the responding private guard having direct contact with the alarm monitoring station so that they can receive regular updates.

[1] This is not to say that mobile apps are exclusive to consumerized alarms. Most conventional systems are now sold with mobile app integration, based on an IP communicator module and a message broker like alarm.com.

[2] Actually this not the case with well-installed conventional alarms, which usually have interior motion detectors not near the entry doors set up as immediate zones meaning that they will trigger the alarm immediately if violated during the entry delay. This avoids a burglar wandering the house during the entry delay period, when motion is expected only near the door. Some systems even correlate motion detectors

to the zone that triggered the entry delay and will alarm immediately if motion is detected near an exterior door other than the one initially opened. But this also assumes that the alarm dealer did a good job designing and installing the system, which cannot be assumed. Consumerized systems usually arent even capable of this kind of configuration, though, as its more complicated to implement and even more complicated to explain to consumers who are designing and configuring their own system.

[3] This might seem like less of a concern since the siren doesnt sound until the alarm goes into the alarm state. There are two problems: first, some consumerized alarm systems play their entry delay warning sound from the controller as well. Second, to minimize nuisance false alarm dispatches most alarm systems dont actually report an alarm event until the siren has been sounding for a certain period of time, sometimes as long as 2 minutes.

[4] Most Abode hardware, and the protocol itself, seem to be white-labeled from a manufacturer called Climax. The fact that they mostly dont design their own hardware only makes it more embarrassing that their software is such a mess. This is quite common among these consumerized alarm systems, though. Look at enough of them and you will start to notice suspicious similarities: almost all of them use white-label hardware for at least the sensors, and some are little more than a new logo on a product thats been around for a while in the EMEA market.

[5] This is basically what happened with WiFi deauth attacks, which went from the topic of security conference talks to a 32 EUR portable device rather suddenly... and that price is from a reputable manufacturer, there are many cheaper options. Similarly the programming interface defect in Onity locks was viewed as being a mostly theoretical problem in the hospitality industry until suddenly people were going through hotels with pocket-sized implementations of the attack. The point I am trying to make here is that the attack is possible but not practical is usually sort of a gamble with the future.