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

2021-10-11 intro to burglary

One of the best-known brands in American burglar alarm systems is ADT. ADT stands, of course, for American District Telegraph. As the name suggests, ADT did not originate as a burglar alarm company. Instead, it started as a telegraph operation, mostly providing stock quotes and other financial information within cities. As happened with many early telegraph companies, ADT became part of Western Union and later part of AT&T. The history of ADT as a telegraph company is not all that interesting, and their telegraphy business is not well remembered today.

The modern ADT story starts, the company history tells us, with someone breaking into the home of one of the founders of one of ADT's constituent companies. This was the origin of the business line we know ADT for today: burglar alarms. While a number of companies have entered and exited the burglar alarm market (including AT&T itself as a separate venture from ADT), none have gained the market dominance of ADT... dominance so great that they lost an antitrust case in the '60s.

Before we get to the history of burglar alarm signaling, though, we should discuss the burglar alarms themselves.

The fundamental concept of a burglar alarm is fairly simple, and might better be explained by analogy to a similar, simpler system. Many industrial machines make use of a "safety string" or "safety circuit." This consists of a set of limit switches or other devices connected in series on things that are safety critical, like access doors. It's all arranged such that, in a "normal" state, the safety string is closed (all of the switches are in their circuit-closed state). If any unsafe condition occurs, such as an access door being opened, a switch opens the circuit. This usually cuts power to the potentially dangerous equipment.

A burglar alarm is simply the extension of this concept to multiple circuits. A set of switches and sensors are installed throughout the protected area. Any of these sensors indicating an "unsecured" state causes an alarm.

In practice, the wiring of burglar alarms is more complex than that of a simple safety string. There are various reasons for this, but the most obvious is the problem of *supervision.* Burglar alarms are designed to operate in a somewhat hostile environment including the possibility of tampering, and in any case insurance companies usually require that they have an adequate "self-test" facility to ensure that the system is functioning correctly during arming. This means that the alarm system needs to have a way to determine whether or not the sensor circuits are intact--whether the sensors are still connected. This is referred to as supervision.

A very common supervision method is the end-of-line resistor. A common burglar alarm

circuit arrangement is the normally closed circuit with 5.6k EOL resistor. In this system, the sensors are each connected to the alarm in series and are normally closed. When a protected door is opened, for example, the sensor opens the circuit which is detected by the alarm controller. An enterprising burglar, though, might realize that they can short the two alarm wires together and thus prevent the circuit ever opening. An EOL resistor complicates this attack by creating a known, fixed resistance at the far end of the sensor circuit.

Let's imagine that the alarm controller functions by measuring the resistance of each alarm circuit (they basically do, but usually instead by putting a fixed current on the circuit and then measuring the voltage drop). If the resistance of the circuit is infinite, it is "open," which indicates an alarm. If the resistance of the circuit matches the expected EOL resistor (say 5.6k but the value just depends on what the alarm manufacturer chose), everything is normal. If the resistance of the circuit is zero (or near zero), the circuit has been shorted... and that can result in either the alarm sounding or reporting of a "trouble" condition.

This isn't the only way to use an EOL resistor. Another approach that is very common with fire alarms is a normally open EOL resistor circuit. In this system, the normal state is the fixed resistance of the EOL resistor, but the "initiating devices" such as smoke detectors are connected between the two alarm wires and actually short them together (creating a zero resistance) to cause the alarm to sound. In this case, an infinite resistance (open circuit) indicates that the circuit has been broken somewhere. In practice the difference between normally-open and normally-closed alarm circuits is more one of convention than technical merit, as both have very similar reliability characteristics. Largely for historical reasons, burglar alarms tend to be normally closed and fire alarms tend to be normally open, but there are many exceptions to both.

In early burglar alarms, this basic concept of measuring the resistance of an alarm circuit to check for a "normal" or "secure" value was very clear. A common vault alarm in the early 20th century had a large gauge showing the resistance of the single circuit and a knob which was used to adjust a variable resistor. To arm the alarm, the knob was turned (adjusting a reference resistance) until the needle fell into the green band, and then the alarm was switched on. The needle leaving the green band in either direction (indicating an open or a short circuit) resulted in an alarm, often by a mechanism as simple as the needle touching a peg (but perhaps also by things like spring-balanced magnetic coils). Modern burglar alarms are mostly just an evolution of this same design, although digital communications are becoming more common.

A burglar alarm usually uses several of these circuits, which are labeled "zones." Zones could correspond to physical areas of a protected building (and sometimes do), but for practical reasons it's very common for zones to correspond more to type of sensor than location. For example, it is very common to have one zone for perimeter detection devices (e.g. window and door closures) and one zone for presence detection devices (e.g. motion detectors) [1]. This is done so that different types of sensors can be armed separately, most often to enable a "perimeter" or "home" or "stay" mode in which the sensors on entry and exit points are armed but the sensors on the interior space are not.

Besides the sensors themselves, another important part of a burglar alarm is a means of arming and disarming it. Due to the lack of practical digital technology, early alarms took a very mechanical approach. A common arrangement in commercial buildings was a two-keyswitch system. To disarm the alarm, a key switch on the outside of the building had to be turned to the disarm position. Then, within a certain time period

(measured by anything from a mechanical timer to a thermistor and heater), a second keyswitch located somewhere in the building had to be turned to the disarm position.

This somewhat complex system is actually very clever. It's quite possible that a skilled burglar will pick, dismantle, or otherwise defeat the outside keyswitch. The interior keyswitch serves as a "what you know" second factor: a burglar, not being familiar with the building's alarm system, would probably not know where the second switch was and would run out of time while looking for it. To improve this mechanism, the alarm panel and second keyswitch (it was usually right on the alarm panel) was often put somewhere non-obvious like a closet off of an office or behind a painting.

This use of two different key switches gets at a fundamental concept in the design of burglar alarm systems. The set of access points (like doors and windows) monitored by the alarm delineates a boundary between the secured space and the unsecured space. Alarm equipment within the secured space gets a certain degree of protection against physical tampering by virtue of its location: it is difficult to a burglar to tamper with something if they can't get to it without setting off the alarm. On the other hand, devices in the unsecured space, such as a keyswitch placed outside, are much more vulnerable to tampering. These devices need some kind of additional protection, or need to have their capabilities limited. The same problem exists with door locks and all sorts of other security systems [2].

In other cases a much simpler and more manual approach was taken. In some early alarm systems, there was no way to disarm the alarm. Instead, the employee opening for the morning would contact the monitoring point and exchange codewords (or otherwise identify themselves), so that the alarm center operator knew to disregard the upcoming alarm. This is actually still a fairly common practice both in military and other high security installations (where the extra manual checks are worth the resources) and in multi-tenant, infrequent access locations like radio towers where it would become frustrating to issue alarm codes to all of the different contract technicians. You will sometimes see signs along the lines of "Call 123-456-7890 before entering," which is a good indicator that this approach is still in use [3].

By the '70s the "alarm code" or "alarm PIN" was becoming the dominant approach, with users expected to disarm the alarm by entering a numeric combination. Modern alarms still mostly rely on this method, although it's getting more common to be able to arm and disarm alarms via the internet or a remote keyfob.

In both the cases of sensors and arm/disarm mechanisms we see that there has not been a great deal of technical progress over the last decades. In general the alarm space is somewhat stagnant, but it depends on the market. Consumer systems are changing very quickly, but in some ways for the worse, as newer consumer alarms are often cheaper and easier to install but also less reliable and easier to tamper with than older systems. No small number of the "ease of use" improvements in consumer alarms are directly achieved by reducing the security of the system, usually in a way that consumers don't clearly understand (more about this later).

Commercial alarm systems, on the other hand, have changed much less. Partially this is because the market is small and somewhat saturated, but partly it is because of the relatively higher security and certification requirements of commercial insurance companies. For businesses, insurance discounts are usually a bigger factor in the decision to install an alarm system, and the insurance companies are usually stricter about requiring that the alarm be certified against a specific standard. The good news is that these standards mean that commercial alarms are usually built on all of the best practices of the '90s. The downside is that the standards do not change

quickly and so commercial alarms do not necessarily integrate modern cryptography or other methods of enhancing security. All in all, though, commercial alarms tend to be both more antiquated and more secure than modern consumer alarms.

This post has really just been a quick introduction to the topic of burglar alarms, giving you the basic idea that they function by monitoring strings of sensors and provide some authenticating method of arming and disarming the alarm. In the future, we'll talk a lot more about burglar alarms: about central monitoring systems (remember ADT?) and about the new landscape of DIY consumer systems, at least. Probably some rambling about different types of motion detectors as well.

[1] There are a GREAT variety of different types of perimeter and presence sensors, and they are all very interesting, at least to me. You may be detecting that technical security is an interest of mine. In the future I will probably write some posts about different types of burglar alarm sensors and the historical evolution they have gone through.

[2] While not as relevant today, this is one of the reasons that alarm keypads are usually placed inside the secured space. In older alarm systems, the keypad sometimes directly armed and disarmed the alarm via a simple electrical mechanism, making it possible to "hotwire" the alarm from the keypad. Placing the keypad inside of the secured space, such that anyone accessing it would have set off a sensor and started the entry delay timer, makes this kind of exploit more difficult by putting the burglar on the clock. In well-designed modern alarms the keypad no longer has the capability to disarm the alarm without the user entering a code (i.e. the keypad sends the code to the alarm panel elsewhere to be checked), but even today we can't take this for granted as some manufacturers have "economized" by putting the entire controller into the keypad.

[3] This is particularly common in telecom facilities because telecom companies have an old habit of implementing a "poor-man's burglar alarm." They would simply connect a switch on the door of the equipment hut to the trouble circuit used to report conditions like low backup batteries and failed amplifiers. That way any unauthorized access would result in a trouble ticket for someone to go out and inspect the equipment. Of course, authorized access just meant calling the maintenance office first to tell them to ignore the upcoming trouble alarm.