

Directions: In this section, you are going to read a passage with ten statements attached to it. Each statement contains information given in one of the paragraphs. Identify the paragraph from which the information is derived. You may choose a paragraph more than once. Each paragraph is marked with a letter. Answer the questions by marking the corresponding letter on *Answer Sheet 2*.

Can Burglars Jam Your Wireless Security System?

- A) Any product that promises to protect your home deserves careful examination. So it isn't surprising that you'll find plenty of strong opinions about the potential vulnerabilities of popular home-security systems.
- B) The most likely type of burglary(入室盗窃) by far is the unsophisticated crime of opportunity, usually involving a broken window or some forced entry. According to the FBI, crimes like these accounted for roughly two-thirds of all household burglaries in the US in 2013. The wide majority of the rest were illegal, unforced entries that resulted from something like a window being left open. The odds of a criminal using technical means to bypass a security system are so small that the FBI doesn't even track those statistics.
- C) One of the main theoretical home-security concerns is whether or not a given system is vulnerable to being blocked from working altogether. With wired setups, the fear is that a burglar(入室盗贼) might be able to shut your system down simply by cutting the right cable. With a wireless setup, you stick battery-powered sensors up around your home that keep an eye on windows, doors, motion, and more. If they detect something wrong while the system is armed, they'll transmit a wireless alert signal to a base station that will then raise the alarm. That approach will eliminate most cord-cutting concerns—but what about their wireless equivalent, jamming? With the right device tuned to the right frequency, what's to stop a thief from jamming your setup and blocking that alert signal from ever reaching the base station?
- D) Jamming concerns are nothing new, and they're not unique to security systems. Any device that's built to receive a wireless signal at a specific frequency can be overwhelmed by a stronger signal coming in on the same frequency. For comparison, let's say you wanted to "jam" a conversation between two people—all you'd need to do is yell in the listener's ear.
- E) Security devices are required to list the frequencies they broadcast on—that means that a potential thief can find what they need to know with minimal Googling. They will, however, need to know what system they're looking for. If you have a sign in your yard declaring what setup you use, that'd point them in the right direction, though at that point, we're talking about a highly targeted, semi-sophisticated attack, and not the sort of forced-entry attack that makes up the majority of burglaries. It's easier to find and acquire jamming equipment for some frequencies than it is for others.
- F) Wireless security providers will often take steps to help combat the threat of jamming attacks. SimpliSafe, winner of our Editors' Choice distinction, utilizes a special system that's capable of separating incidental RF interference from targeted jamming attacks. When the system thinks it's being jammed, it'll notify you via push alert(推送警报). From there, it's up to you to sound the alarm manually.
- G) SimpliSafe was singled out in one recent article on jamming, complete with a video showing the entire system being effectively bypassed with hand-held jamming equipment. After taking appropriate measures to contain the RF interference to our test lab, we tested the attack out for ourselves, and were able to verify that it's possible with the right equipment. However, we also verified that SimpliSafe's anti-jamming system

works. It caught us in the act, sent an alert to my smart phone, and also listed our RF interference on the system's event log. The team behind the article and video in question makes no mention of the system, or whether or not it detected them.

- H) We like the unique nature of that software. It means that a thief likely wouldn't be able to Google how the system works, then figure out a way around it. Even if they could, SimpliSafe claims that its system is always evolving, and that it varies slightly from system to system, which means there wouldn't be a universal magic formula for cracking it. Other systems also seem confident on the subject of jamming. The team at Frontpoint addresses the issue in a blog on its site, citing their own jam protection software and claiming that there aren't any documented cases of a successful jam attack since the company began offering wireless security sensors in the 1980s.
- I) Jamming attacks are absolutely possible. As said before, with the right equipment and the right know-how, it's possible to jam any wireless transmission. But how probable is it that someone will successfully jam their way into your home and steal your stuff?
- J) Let's imagine that you live in a small home with a wireless security setup that offers a functional anti-jamming system. First, a thief is going to need to target your home, specifically. Then, he's going to need to know the technical details of your system and acquire the specific equipment necessary for jamming your specific setup. Presumably, you keep your doors locked at night and while you're away, so the thief will still need to break in. That means defeating the lock somehow, or breaking a window. He'll need to be jamming you at this point, as a broken window or opened door would normally release the alarm. So, too, would the motion detectors in your home, so the thief will need to continue jamming once he's inside and searching for things to steal. However, he'll need to do so without tripping the anti-jamming system, the details of which he almost certainly does not have access to.
- K) At the end of the day, these kinds of systems are primarily designed to protect against the sort of opportunistic smash-and-grab attack that makes up the majority of burglaries. They're also only a single layer in what should ideally be a many-sided approach to securing your home, one that includes commonsense things like sound locks and proper exterior lighting at night. No system is impenetrable, and none can promise to eliminate the worst case completely. Every one of them has vulnerabilities that a knowledgeable thief could theoretically exploit. A good system is one that keeps that worst-case setting as improbable as possible while also offering strong protection in the event of a less extraordinary attack.
36. It is possible for burglars to make jamming attacks with the necessary equipment and skill.
37. Interfering with a wireless security system is similar to interfering with a conversation.
38. A burglar has to continuously jam the wireless security device to avoid triggering the alarm, both inside and outside the house.
39. SimpliSafe provides devices that are able to distinguish incidental radio interference from targeted jamming attacks.
40. Only a very small proportion of burglaries are committed by technical means.
41. It is difficult to crack SimpliSafe as its system keeps changing.
42. Wireless devices will transmit signals so as to activate the alarm once something wrong is detected.

43. Different measures should be taken to protect one's home from burglary in addition to the wireless security system.
44. SimpliSafe's device can send a warning to the house owner's cellphone.
45. Burglars can easily get a security device's frequency by Internet search.