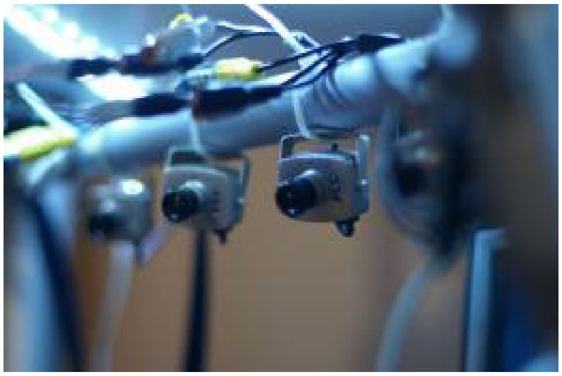
PHYS ORG

Seven myths about physical security

October 27 2010, By Louise Lerner, ANL



Testing security cameras, just 4 for now, temporarily mounted with cable ties. Image credit: Jaymis Loveday.

The high-tech access control device was secure, sophisticated, and complex; it was intended to protect nuclear materials and other important assets. But security experts at the U.S. Department of Energy's Argonne National Laboratory defeated it with parts from a Bic pen.

Argonne security experts have revealed the dirty secrets behind electronic voting machines, "high-security" electronic locks, iris and fingerprint scanners and even GPS navigation systems.

Roger Johnston heads Argonne's Vulnerability Assessment Team (VAT), which spends their workdays trying to defeat security devices.

Physical security—the art of protecting tangible assets—is the counterpart to cyber security, which seeks to safeguard data. Physical security can take the form of walls, locks, guards who stand watch at nuclear facilities, fingerprint scanners and metal detectors, and even the GPS system that tracks trucks full of nuclear material. It is high-tech, low-tech, often ancient, and usually overlooked.

Physical security is harder, too, in some ways: attacks are rarer, but often far more devastating. Cyber attacks happen millions of times a day and are often costly, but don't result in loss of human life. On the other hand, physical security defenses aren't tested very often, but when they are, the results can be catastrophic.

Johnston is fond of the saying, "Real security is thinking how bad guys would think." His work, which often involves advising both government and private companies on security, has led him to create a set of maxims about what is and isn't good security.

Here are seven commonly held security perceptions that he believes don't hold up under pressure.

MYTH: Electronic voting machines are reliable and secure.

It took Jon Warner, a systems engineer on Johnston's team, less than two hours to devise and rig an electronic voting machine to swap the votes for two candidates.

This follows another of Johnston’s security tenets: The more sophisticated the technology, the more vulnerable it is to primitive attack.

"Engineers developed this machine to be resistant to a high-tech attack—they test whether the microprocessor can be hacked. But they don't test whether someone, including the voter, could pop open the panel with a screwdriver and cross a few wires," Johnston said. "The machine is unaware that it's been opened; it has no sensor. Almost anyone could do it."

The machines could be sabotaged during storage periods between elections, or while they're trucked from location to location. A simple addition let Johnston's team turn the cheating on and off with a remote control from up to half a mile away—so the machine could pass tests in the morning and after the election, but be triggered to cheat during actual voting.

According to Johnston, that kind of rigging could affect the outcome of a race. "Statistics suggest that elections are getting closer and closer," he said. "Elections are routinely won now by just a few percentage points, and rigging machines in a few districts could certainly make a difference there."

Johnston and his colleagues on the VAT believe the problem can be fixed simply, by making sure each voter sees a printout that confirms how he or she just voted. Election officials don't like it because printers tend to jam, slowing the voting process, but it's more secure. Voting machines could also be equipped with sensors that recognize tampering.

MYTH: GPS is totally accurate and secure.

GPS is a success story of engineering and publicly funded research, and it has saved many lives and lost drivers. But it's also an unsecured technology.

The receivers in your car's GPS navigation system, and most other forms of civilian GPS, are easy to attack, Johnston said. His concern is not the signal to the device being blocked or jammed; the user would notice such an attack because the device would stop working.

"What we're worried about," said Johnston, "is a more elegant, malicious attack called GPS 'spoofing.' That's when an attacker feeds false information to the GPS, making it think that it's in another location—and you'd never know."

Spoofing is possible because the GPS signal received from space is actually quite faint. An attacker broadcasts a fake GPS signal with a higher signal strength, and the receiver picks up that signal instead. Such fake signals can be easily generated by user-friendly GPS satellite simulators that can be purchased, rented or stolen, and are not export-controlled.

Johnston and his team helped to identify two threats to our national security that could arise from this vulnerability. One is that a GPS attack could shut down our informational infrastructure. "Many of our national networks —telecommunications, utilities, computers, financial transactions—get their critical time synchronization from GPS satellites in space," Johnston said. "And since it's very easy to spoof a GPS and throw off that synchronization, it's potentially very easy to crash those networks—in milliseconds."

GPS vulnerabilities also present a threat to shipments of valuable or dangerous cargo, such as nuclear materials. Because they use civilian GPS to navigate, they could be hijacked—led down the wrong road into an ambush, for example, all while reporting back to headquarters that the truck is on course. The U.S. Department of Defense uses a specially encrypted GPS for weapons applications, but many forms of nuclear material often don't fall under weapons qualifications, so they aren't allowed to use the encrypted network.

"It's a little unfair to blame the civilian GPS system, because it was never meant for security," Johnston said. "But it's being used that way."

To patch these flaws, Johnston and his team have come up with several inexpensive ideas for improving GPS security. Most fixes involve retrofitting GPS receivers; they can be modified to notice if a signal is too strong—and thus probably fake—or to track satellites by their identification codes.

MYTH: People are good observers.

We often rely on humans—whether security guards or passersby on busy trains, subways and streets—to notice something suspicious and alert the authorities; but this might not be as effective as we think. "People consistently overestimate how good they are at observing," Johnston said.

For instance, Harvard and University of Illinois researchers performed a classic psychology study in which fully half of observers, instructed to count the number of times a basketball changed hands in a video, completely miss a man in a gorilla suit who walked across the court in the middle of the game, pounded his chest and walked out.

Why don't half the observers see the gorilla? "The gorilla doesn't make any sense in the context of a basketball game, so the brain ignores it," Johnston said. Psychologists call it perceptual blindness. The ability to concentrate on a task and ignore distractions is crucial while studying for a test, but becomes a handicap when noticing an odd detail could prevent a serious attack.

This has important implications for day-to-day security—not only because you might tune out the man acting strangely in a crowd, but also for security guards, who watch the same rooms, gates or camera monitors for eight to 10 hours a day. Johnston suggested that mental exercises could help guards prepare for the unusual; or motion-detectors or other technology can support a guard's eyes.

MYTH: Polygraph tests catch the bad guys.

According to Johnston, no major U.S. spy has ever been caught with a polygraph test. In fact, many later-identified spies sailed through polygraph tests, often multiple times.

Why do lie detectors fail? Johnston suggested that narcissism is a surprisingly good shield against polygraph tests. "Spies often believe their own lies," he said. "They believe, 'I deserved to steal this information.' If you believe what you did is right, then the physiological and body language signs don't show up."

In addition, reading body language and physiological reactions is a tricky—and unreliable—art, and polygraph operators are often only required to take a week of training. "In many states, a barber needs more training to become licensed than a polygraph examiner does," Johnston said.

Scientists are studying whether new equipment that maps brain activity, such as MRIs and electroencephalograms (EEGs), may be more effective than polygraphs; but the results are as yet unclear.

MYTH: Fingerprint and eyeball scanners are more secure than traditional methods.

Fingerprint and eyeball scanners fall under a category called biometrics: using unique biological "signatures" to restrict access to only a few people.

But just as in the case of voting machines, high-tech security is often easier to defeat than traditional low-tech security. The more complex a machine, the more ways there are to attack it. And while engineers may design the scanner so that a direct attack is difficult, an attacker could conceivably bypass the technology itself by, for example, loosening the back panels.

"The problem is, most biometric devices don't have intrinsic security built into them at all," Johnston said. "It isn't that they can't provide good security; it's that they don't, which is because no one adds effective sensors to the machine to let it know if it's been tampered with."

Other human errors undermine the security of fingerprint scanners. "You get what is called the Titanic effect," Johnston said. "Everyone thinks it'll never sink and that it can't be beat, so no one has to think about it." Human operators also don't often understand the devices, which makes recognizing their errors difficult.

Johnston belives that the manufacturers of biometric security devices can boost their effectiveness by adding sensors that would recognize tampering.

MYTH: Drug tests are fully secure and accurate.

Johnston and his team looked at 23 security products as well as security protocols widely used to protect urine samples for drug testing, and found they can all be compromised. “In our view, there's no security there to speak of," he said.

The problem with current protocols, according to Johnston, is that security devices focus on preventing tampering with the sample after it has been collected. However, the reverse possibility—an innocent athlete or employee whose sample is spiked on purpose—is rarely considered.

Protecting the empty vial prior to use is just as important, Johnston said, especially because the amount of material needed to generate a positive test is so infinitesimal that it could be invisible to the human eye. An undetectably tiny amount could be added to the vials to contaminate the urine sample ahead of time.

After the sample is collected, the vial still isn't fully protected. "The main post-collection security is a label that you slap over the lid of the vial—a vial that's made out of polyethylene, one of the slipperiest plastics anywhere," Johnston said. "Sometimes the labels peel right off the vial on their own. That's no security."

In addition to determining athletic and job eligibility, substance tests are also used after a transportation accident or industrial failure to test for substances in the blood of drivers or engineers. These, too, can be easily faked.

"This is an outrageous situation for people who can lose their jobs over a drug test," Johnston said. "You're talking about the reputation, the livelihood, the life of this athlete, engineer or employee. A positive, even if it's later proved false, can be fatal to a career. This has to be done right."

MYTH: Security cameras reduce crime.

"This is one aspect of security that's fairly well studied," Johnston said. "In Britain, there are about 4.4 million video cameras, and they don't stop crime. Particularly not violent crime."

In studies, street cameras are sometimes found to reduce nonviolent crime, such as vehicle break-ins; but just as often, crime rises in the next block over—a phenomenon called displacement.

Cameras are not a deterrent, Johnston said, because most violent crimes are crimes of passion. The possibility of a video camera isn't enough to stop someone fueled by rage.

What cameras are useful for is prosecution. "It's often used to prove that a crime took place," Johnston said. That is, if a defendant claims he didn't have a gun during the robbery, this can be disproved by camera footage. But in general, security camera footage tends to be supporting evidence at best. Video resolution is often very poor—insufficient to positively identify a criminal. It may give detectives clues to a person's height or clothing, but facial recognition is often problematic.

"Finally, it's also a myth that a camera replaces a cop," Johnston said. "A cop on the street is worth way more than a camera."

Though the human eye may be flawed, technology isn't about to replace it completely anytime soon.

Source: Argonne National Laboratory

Citation: Seven myths about physical security (2010, October 27) retrieved 5 May 2024 from https://phys.org/news/2010-10-myths-physical.html