It's a given that shadowrunners and other criminals will, at some point, need to smuggle weaponry into a building and past security checkpoints. **Magnetic anomaly detectors (MADs)** detect metallic substances for the purpose of finding concealed weaponry. (Naturally, MADs do not work against non-metallic substances like wood, stone or plastic.) To determine if the detector finds a weapon, make a test using the device's rating as the dice pool; a single hit will detect any ferrous-metal weapons or objects (guns, knives, etc).

Millimeter wave detection systems, also known as **cyberware scanners,** process video taken in the millimeter wave spectrum to identify the energy signature of cyberware and concealed items (specifically weapons) on a person. These devices can "see through" thick layers of clothing and other concealment to identify items from a distance of 15 meters away. To determine if the detector scans cyberware or a prohibited item, roll the Device rating and compare the hits scored to the thresholds given on the Cyberware Scanner Table. Millimeter wave scans can detect any non-biological item by its shape and composition, assuming the item is listed in the device's database. If the threshold is reached, the scanner detects the item/implant and notes its general locations and type; additional hits provide more detail (function, model, grade, etc.).

Locks

Nearly everything with any worth will be locked away.

Key locks are the simplest kind, involving the use of tumblers and metal keys or combination code dials to open doors instead of cards or some other device. They are also not in very common use due to reliance on more sophisticated means of security, but some places (like private safes or low-end businesses) may still use them out of nostalgia, because they can't afford better, or because rarity equates better security. Defeating a key lock requires a Locksmith + Agility (variable, 1 Combat Turn) Extended Test, with threshold determined by the quality of the lock. Autopickers (p. 326) add their rating in dice to this test; their rating may also be used in place of Lockpicking skill.

Transponder-embedded keys contain a calibrated resistor that completes a circuit in the lock. In order to pick such a lock by hand, an electronics kit is needed to generate the appropriate electrical characteristics. This requires a successful Hardware + Logic (Lock Rating, 1 minute) Test at the same time the lock is picked. If the same character is picking the lock and calibrating the electrical feed, apply a –2 dice pool modifier to both tests.

Maglocks

Powered magnetic locks are widespread in 2070, and come in a wide range of sophistication. Maglock "keys" can be physical (keypad, swipe card, proximity card, memory string), biometric (see below), or any combination thereof. Maglocks are often accessible via the local network (wired or wireless) and may be monitored by a security hacker/rigger. Maglock systems often log all usages, keeping track of the time, date, and identity of each user.

The first step to bypassing a maglock is to remove the case and access the maglock's electronic "guts." This requires a successful Hardware + Logic (Maglock rating x 2, 1 Combat Turn) Extended Test. If all else fails, the case can be smashed or shot off; treat the case as if it has a Barrier rating equal to the maglock rating. Overzealous attempts to break the case may harm the electronics inside. Re-assembling the case afterwards requires the same test.

Some maglock systems come equipped with **anti-tamper systems,** rated between 1 and 4. In order to bypass the anti-tamper circuits, an additional Hardware + Logic (anti-tamper system rating) Test must be made. If this fails, an alarm is triggered.

Keypads utilize an access code (often different access codes for different users). Unless the code is known, defeating a keypad requires rewiring the internal electronics. This means cracking open the case (see above) and then rewiring the circuits—another Hardware + Logic (Maglock rating x 2, 1 Combat Turn) Extended Test. A sequencer (see p. 327) may also be used instead; make an Opposed Test between the sequencer and maglock ratings. If the sequencer wins, the maglock opens. (Note that the case must still be opened for a sequencer to be applied.)

Cardreaders verify the authenticity of swipe cards or RFID proximity cards. They can be defeated using the same method as for keypads—by removing the case and tampering with the works. Maglock passkeys (p. 326) may also be used to defeat cardreaders, and don't require breaking the case open. If a valid keycard is acquired, it can be copied with a keycard copier (p. 326) in order to create a forged keycard. Make an Opposed Test between the passkey/forged keycard rating and the maglock rating. If the passkey/forged keycard wins, the maglock opens.

Biometrics

Biometric systems work by measuring a "print" (finger, retinal, voice, etc.) from the user and checking the measured print for matches in a database of authorized prints. This means biometric scanners almost always have a local network connection (wired or wireless). Because the print-matching takes place in a remote database, biometric scanners tend to be harder to bypass. If the characters can access the database (whether by hacking or other means), they can modify it to include their own print records as authorized personnel. This is a risky route, however, as the system will retain their records and log what they accessed (unless those records are also modified later).

Print scanners scan fingerprints, palm prints, retinal prints, or even the pattern of blood vessels in the face or palm. One method to defeat a print scanners is to coerce an authorized user to apply their prints. Alternately, a synthetic print glove-like membrane (a "sleeve") can be manufactured for fingerprints and thumbprints with a cellular glove molder (an authorized print is necessary to copy from, see p. 326). Retinal prints may also be duplicated with the retinal duplication cybereye accessory (p. 333). If a fake print is used, make an Opposed Test between the duplicate and the maglock rating; if the fake wins, the maglock accepts it.