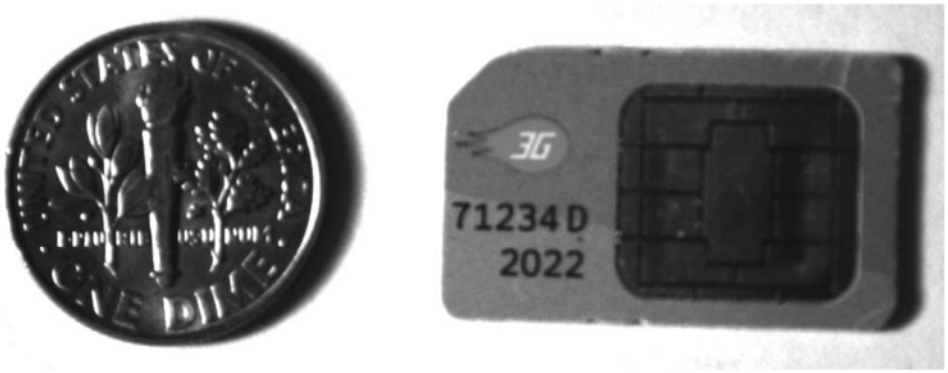

Figure 2.9: A SIM card used in a GSM cell phone, together with a dime to show size. Photo by Dan Rosenberg included with permission.

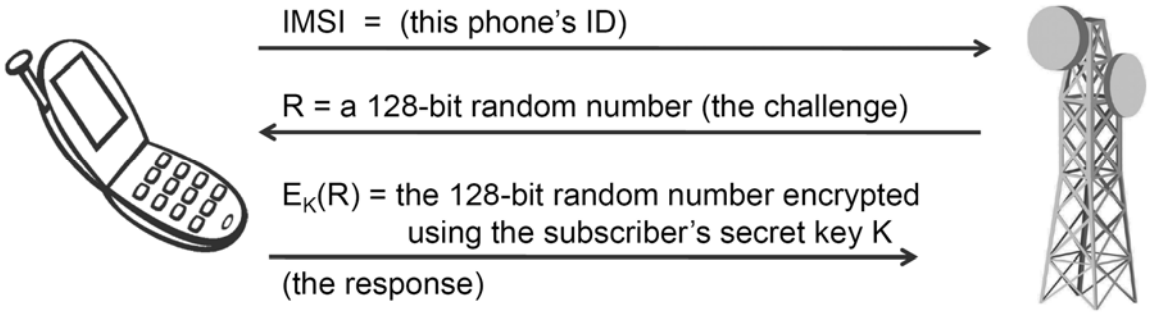

Figure 2.10: The challenge-response protocol between a cellphone (together with its SIM card) and a cell tower. The security of this protocol is derived from the fact that only the phone and the tower should know the subscriber's key.

RFIDs

Radio-frequency identification

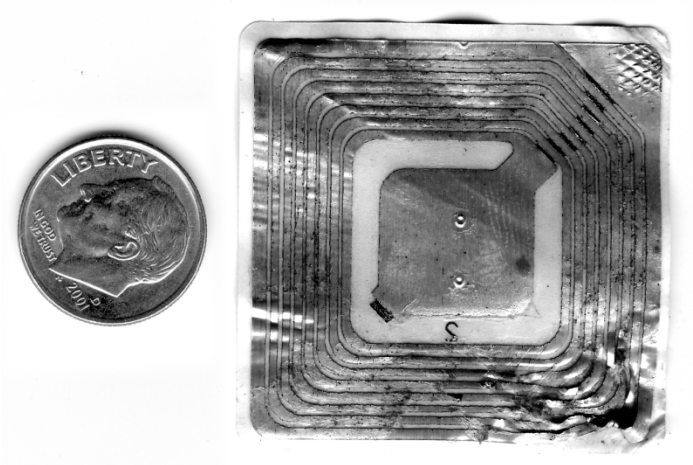

Figure 2.11: An RFID tag, taken from a DVD package, together with a dime to show size. Photo by Dan Rosenberg included with permission.

Figure 2.12: An e-passport issued by the United States of America.

Biometric identification

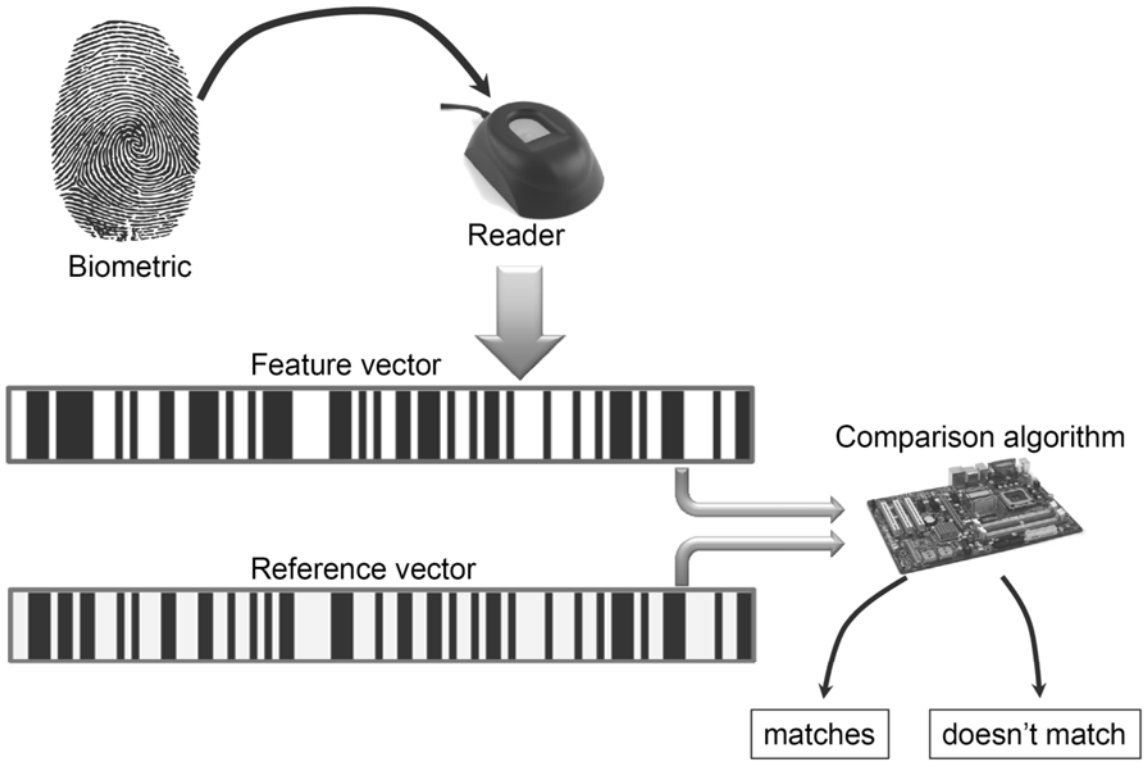

Figure 2.13: The verification process for a biometric sample. A biometric sample is converted into a feature vector and that vector is compared against a stored reference vector. If the similarity is good enough, then the biometric sample is accepted as being a match.

8.3. Direct attacks against computers

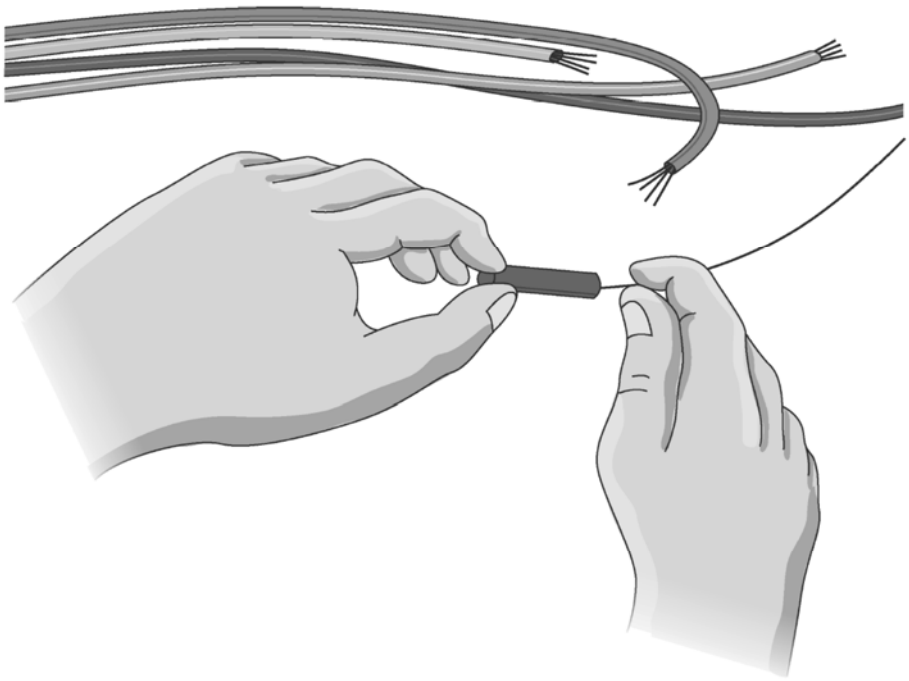

Figure 2.14: Wiretapping.

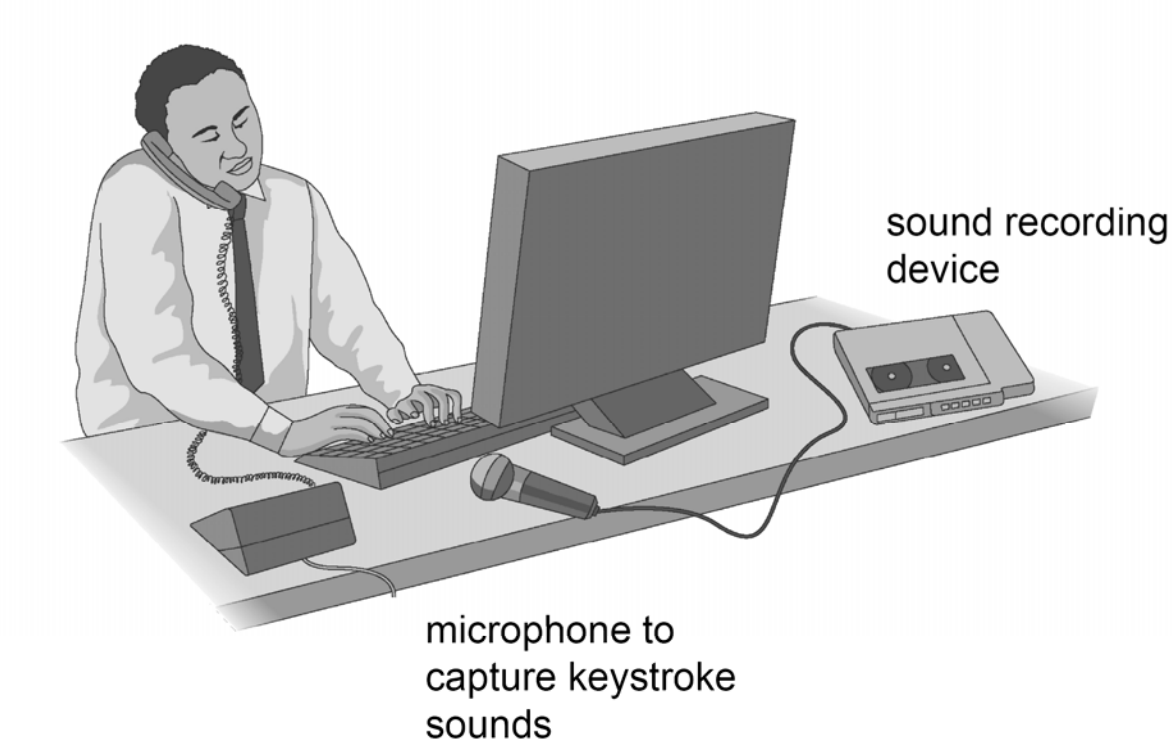

Figure 2.15: A schematic of how a keyboard acoustic recorder works.

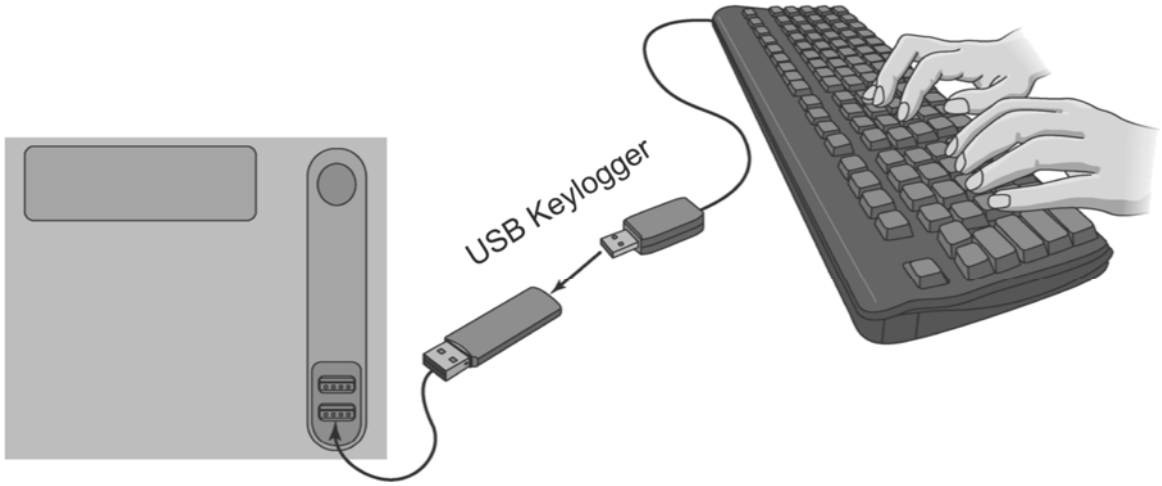

Figure 2.16: A schematic of how a USB keylogger works.

Emanation Blockage

Figure 2.17: An example Faraday cage. (Image by M. Junghans; licenced under the terms of the GNU Free Documentation License, Version 1.2.)

Computer Forensics

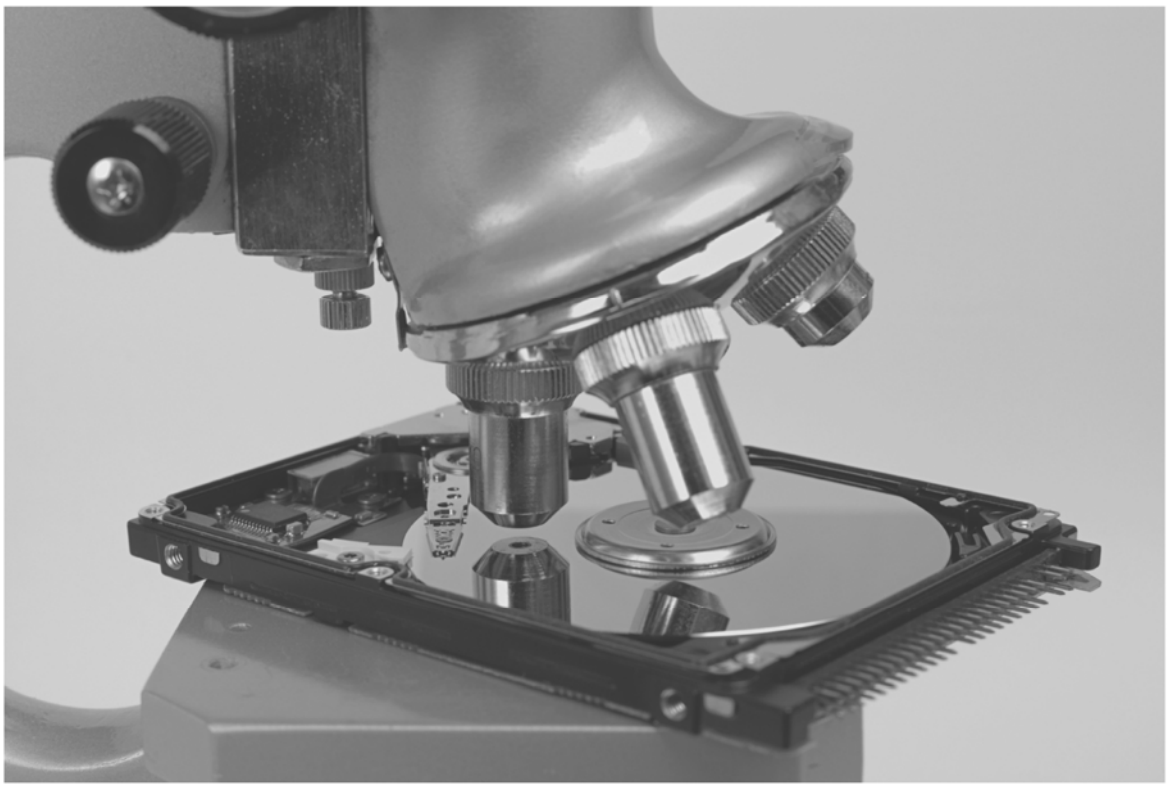

Figure 2.18: Microscopic inspection of a disk drive.

Physical Intrusion Detection

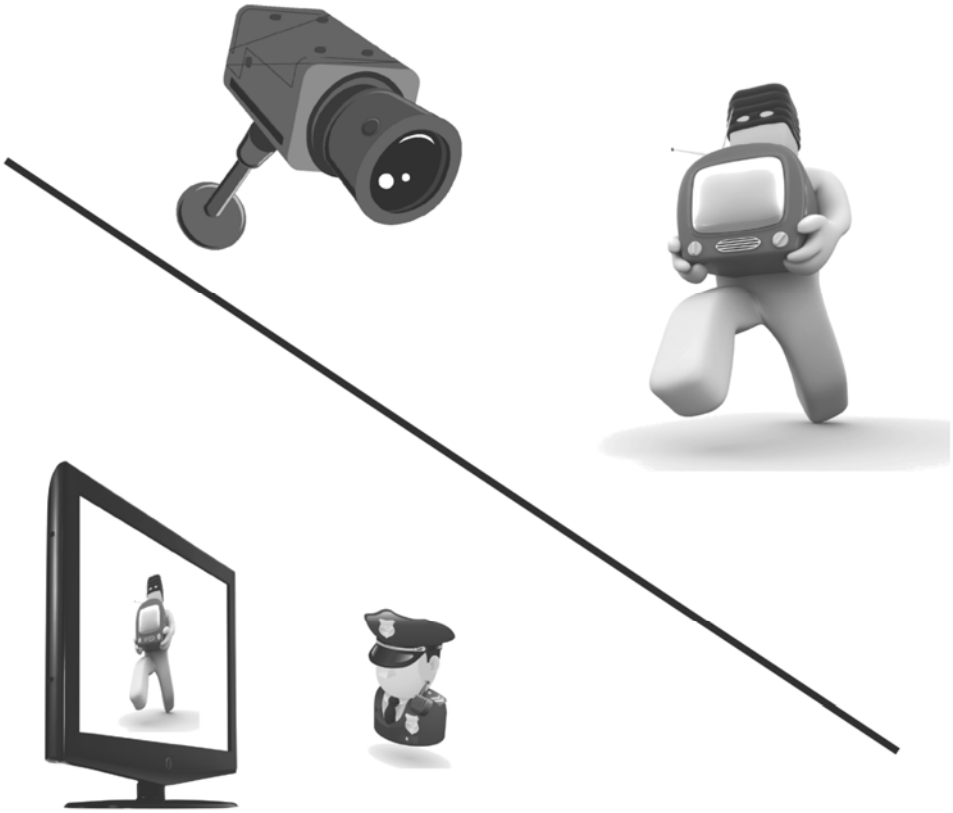

Figure 2.20: The components in a video monitoring security system.

Social Engineering

Figure 2.21: An example of a social engineering attack on a security guard: "Thanks for understanding about me leaving my ID card at home."