Interview with Keith Crowdy, security consultant, 9 July 2003

Most biometric security systems use either retina or fingerprint details for ID.

Fingerprint systems no longer use cameras. They detect the pattern of fingerprints by minute electrical differences between ridges and valleys. They match 25 points of the fingerprint. Therefore they cannot be fooled by a gelatin finger, which has no electrical characteristics.

The weakness of most security systems is that they use the corporate network, which has not been designed to be secure. You can access the corporate network via a Speedlan from outside the premises. If you have the correct passwords you can impersonate the Administrator.

You can capture several hours of uneventful images from a CCTV camera and replay them through the system the following night. The monitors will show empty rooms even when you are in the building.

A superior system will have an independent security network that cannot be accessed by the IT Administrator, only by the Security Administrator. Both CCTV and access control would be functions of the security network. Passwords would be changed regularly, so that insecure passwords would become obsolete quickly.

With a smart card system, the central processing unit does not need to retain people's fingerprints. Instead, the fingerprint information is on the chip in the smart card, and the computer merely checks that the finger on the screen matches the information in the chip.

Potential burglars could buy cards and a smartcard read-write device, and programme the cards with their own fingerprints; so the card manufacturers incorporate a site-specific code, so that only cards coded for this site can be used.

A thief would have to steal a site-specific card from an authorised user and overwrite it with his own fingerprint information, using a read-write device bought from a shop. Question: is the fingerprint information encoded?

CROWDY

Retina & fingerprint

Dual use cameras

Take an algorithm of 25 point of the fingerprint.

corporate network not designed to be secure. Security a
built-in.

TCP/IP protocol for communication

Use specialized in client IT network - need password

CCTV uses the corporate network.

Every network has static and dynamic IP addresses

All static addresses recorded in database which is on the
IT system

Scan network, search & know if previous footage.

(camera house
today)

Search - picture number (in each room of

an agency - turn date stamp off.

(Administrator)

Readers connected to door controller

CCTV connected to Administrator work station

only administrator has access to the database.

Change passwords regularly.

Ensure no additional system administrators have been put on the system

---

Separate security network.

Smart card chip

Smart card read - write data for a security wristband.