Over the last couple of days a small furore has erupted over allegations a News Corp subsidiary, NDS, has been hacking the pay-TV smartcards of News Corp’s competitors, and even News Corp’s own companies – allegations that NDS vigorously denies.

I’m not going to speculate on the reasons why a supplier of Conditional Access Systems – the technology that allows paid-TV providers to restrict access to their broadcasts – would want to undermine the security of their own product; but I am going to discuss how such systems work, and how secure they are.

A Conditional Access Module (CAM) is a combination of encryption keys, smartcards and electronics and computer code inside a satellite or cable-TV receiver (or “decoder”).

The pay-TV provider encrypts the digital signal sent to the subscriber with an encryption key. The subscriber plugs a smartcard into his/her decoder, which decrypts the signal so programs and films can be displayed on the screen. Some decoders have the smartcard built-in already, so there is no external slot.

The smartcard is a plastic card with a chip - much like a modern credit card. You can see electrical contacts on the chip. When the card is inserted, the chip is plugged into the decoder, allowing the CAM to get the decryption key. Other information is also stored on the chip – subscriber ID, subscription details, billing details, censorship filters and so on.

We don’t really know what’s there unless we hack into the chip, because it’s all kept secret. Each chip will have it’s own non-volatile memory (requires no battery), computer programs and a small central processing unit (CPU).

The security of the system depends on a few things:

- secrecy of the encryption algorithm
- secrecy of the keys
- secrecy of the hardware.

So let’s start with the algorithm. An algorithm is a recipe for doing something – in this case, for scrambling and descrambling the digital signal.

Some CAM providers write their own algorithm, and depend on it remaining a secret. That’s a bit like hiding your door key inside a brick or under a flower pot – once the secret (that the key is in the brick) is discovered, you have no security. DVD security works this way.

A much better approach is to keep the key with you (a secret key). Everybody knows how your door security works (you put the right key in the lock and turn), but that only works if you have the key. If your lock (algorithm) is faulty, you’ll find out quickly enough and replace the lock. Of course, Pay-TV subscribers would have to remember the key, and have to enter it into their decoder - very inconvenient, but very safe.

Foxtel uses Irdeto 5 CAMs. These use 3DES encryption - a reasonably complex encryption algorithm that’s difficult to crack without employing lots of supercomputers. 3DES is a known algorithm - it has been tested for years and, if implemented correctly, will be safe.

And the security of the decryption key? That’s stored on the chip in the smartcard. Not so good. Just like hiding it inside a (very thin) brick. 3DES is a symmetric-key algorithm, which means you use the same key to encrypt and decrypt. If hackers can open up the card and get to the key, they can extract the key and use it to make cloned cards.
This leads us to the secrecy of the hardware. Four years ago, Wired magazine posted a YouTube video (see below) showing Chris Tarnovsky demonstrating how to extract the chip from a smartcard, and access the electrical signals.

Reprogramming the card to display its stored data (including the decryption key) is the next step. Modern cards are better, but the techniques for getting into them are also better.

It’s not even necessary to open up the card. Many digital TV watchers use techniques such as card sharing or internet key sharing to spread the cost of a Pay-TV subscription among tens or hundreds of people.

And you can buy blank smartcards online from places such as Alibaba.com for a few cents each. There are also dedicated forums online to help would-be criminals access satellite TV and Pay-TV without a subscription.

Just Google terms such as Irdeto 5 hacks, Sat Universe and MOSC (Modified Original Smart Card).

So just as with modding Xboxes (circumventing the built-in security mechanisms of the Xbox and Xbox 360 videogame consoles), rooting Android (gaining “superuser” permissions to your Android device’s software) and jailbreaking iPhones (gaining root access to Apple’s operating system), pay-TV piracy/hacking is happening now.

The information is out there and is easy to access. Of course, anyone attempting to use the information has to be technically capable and adventurous.

Is it being done on an industrial scale? Perhaps in places such as China or South America. A lot of the hardware which enables or supports unlawful access to IT systems (e.g. ATM card skimming – the illegal copying of information from the magnetic strip of a credit or ATM card) appears to be coming from those regions.

The Chinese government is trying to stop hacking and the systems which support it. My opinion is that the skills required (to hack these smartcards) are beyond most wannabe pirates and hackers.

Besides, it’s much easier just to install the peer-to-peer file-sharing protocol BitTorrent and download any program or film you want.