Ken Follett_Private

From: Neil McDonald [Neil.Mcdonald@bioscrypt.com]
Sent: 13 July 2003 15:42
To: Crowdy Keith @Consult
Subject: RE:

Hi again,

Let me take your points in order...I will use the colour Red. Hopefully you can see it by the time it gets to you...

-----Original Message-----
From: Crowdy Keith @Consult [mailto:Crowdy.Keith@tpsconsult.co.uk]
Sent: 10 July 2003 07:58
To: 'Neil McDonald'
Subject: RE:

Neil,

No its nothing to do with GCHQ it is purely Ken Follett. I went to see him yesterday and he has started to write the book, it should be on the shelves around Xmas 2004.

He really want to be able to defeat a biometric system in the book. I am struggling a bit to see how he is going to achieve this, but it is quite good fun looking into it.

If you don't mind I would like to use your brain again.

Could a possible scenario like this work:

Using your system (V-smart), a blank card is stolen from the stock supplied to the client.
There is no need to steal a blank card. As long it was a fairly standard Mifare or iClass card, or Legic (for TSSI readers) a new card from anybodies stock will do. You could even attend a trade fair and scrounge one from the Gemplus or HID stand! However, using a new card means that you will have to guess which ID number to use. It is this ID number that is required by the controller.

The thief acquires a V-smart-g reader admin kit etc and programs the card up to work on his system.
Yes, this is easy enough and would be necessary. It is not too expensive either. (<$1000 US).

The thief then steels a real programmed card from an authorised employee.
Ah ha, this is a much better idea than taking a new one from stock or directly from the manufacturer as it will have the ID number and the Site Code in there.

He disables (damaging it) the smart chip on the stolen employee card. he disables (damaging it) the prox part of the previously blank card
No, I wouldn't damage them. You would never be able to repair them and they simply wouldn't work. The small copper coil that is around the outside edge of the smart card (inside the two layers of plastic sandwich, see: http://www.gemplus.com/basics/what.html <http://www.gemplus.com/basics/what.html> also www.hidcorp.com <http://www.hidcorp.com>) is connected with fine wires to the chip inside the card. The coil needs to be energised by the reader so that electricity flows to the chip and the chip can respond to the reader request for information etc. (it is a bit like your electric toothbrush being recharged without any electrical contacts.

If he then shows the two cards to the site reader am I right in thinking that:
1. the finger print would be read and confirmed as correct . Nope, broken

cards wouldn't do anything, see above!
2. the stolen prox reader would be programmed to allow access.
Errr...nope!

OK what's wrong with the theory???

Keith

If Follet insists on getting in the hard way and he doesn't want to bribe an insider to register him on a controller and issue him a card of his own (the usual way) or he doesn't want to cut the wires to the mag-locks (might set an alarm off on a very good system but wouldn't on most...)...then, he will need the 'site code' for the buildings in question.

He will need the site code to unlock the secrets of his stolen smart card. However, he hasn't got very long to do it as the card will probably be reported stolen and the site keys changed. Unless he chooses a part time worker or someone who is on holiday! However, some site keys are changed daily without staff realising. There is a 'primary' and 'secondary' site key. You can set the readers to swap them during set periods. If the stolen card wasn't used during that period, it wouldn't learn its new site key.

There are two ways of getting a site code...bribe someone....or get into the security office and look for it. It is bound to be written down somewhere....or perhaps the lazy company didn't even bother using a site key!

Another way is to use the demo reader that you have just bought and experiment with different site codes. Try number 1, 10, 100...obvious stuff like that. When you have found the correct site code, the stolen card will now work with your reader! You could automate this procedure by buying our SDK (developers kit) and writing a routine to constantly change the site key, then test the card. Once into the card, simply substitute your finger with the finger that is already in there.

This is where you have to choose your stolen card carefully! A part time cleaner may only have access rights between certain hours. In fact the controller might be set to lock everyone out at certain hours. The only one who wouldn't be locked out is the caretaker or security officer. Take his card then, assuming you want to go in after dark?

If you want to be really clever, you could store the correct persons template on your PC. Commit the crime and then take out your template and put back the persons template and the return the card to wherever you got it. This would eliminate one source of investigation as the controller will have registered the entry of that person etc...

Another possibility is to remove the reader that is on an obscure door and replace it with the one that you just bought. When people go to use it, it won't work and will be reported. The security staff will be mystified and the supplier will be called out. This could take ages. I don't suppose that they will check the serial numbers!

The stolen reader will hopefully retain its memory in flash without power. You could use this reader to create cards but you will still need an employee card to figure out which ID number to use. However, you might set an alarm off if the reader was connected to a decent controller that 'pings' the reader periodically to see if it was there.

Even easier still...if it was an Identix V20 installed on a single door with no controller, then it is highly likely that the internal relay is used to open the door. Simply break open the casing, look at the PCB where it says 'relay' next to the edge connector and apply 12V. The door will open.

I'm sure there are other ways to fool other readers....but this is a good start!

Hey, and don't quote me on any of this!

Neil.