

Re: Questions on GSM Penetration test

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-01/0083.html>

From: Tom Buelens (email@tombuelens.com)

Date: 01/27/02

From: "Tom Buelens" <email@tombuelens.com>

To: "M Lister" <m1ist@m-net.arbornet.org>

Date: Sun, 27 Jan 2002 22:00:25 +0100

> *What would you mean by "peel off"? Would that be some kind of physical
> tampering? Most smart cards often have some kind of "Tamper Resistant
> Sealing". Also if you try to peel of the adhesive coating, you will most
> probably break the delicate fuse wire which most Smart Card companies run
> in that adhesive coating, thereby making the whole smart-card completely
> useless.*

"The Netherlands Organisation for Applied Scientific Research" has the tools for 'peeling' of the chip layer by layer (thus not the card). Again I do not know the exact technology they use but it is not just your ordinary knife and screwdriver. More like elektron microscope and the likes. And I do not think they are the only ones on the planet who can.

In this fase they are not interested in the working of the whole device as such. They just take the whole thing apart and 'write every thing down'.

Later they reconstruct the device in simulators, like putting it in Orcad, and then the creative thinking process starts, I guess.

> *Tom, if what you are saying is correct, people can make large amounts of
> money, just copying smart cards with applications like "Pre Paid Telephone
> Cards", "Electronic Purses" etc.*

>

So if you know how a device works you know how to abuse it.

IMHO that sort of thinking is what the US calls DMCA. And that is just not right !

Remember "Security is a proces." (c) Bruce

If the weakest link of your chain is a badly designed smardcard then what you are saying might be right but a simple trustrelationship between customer and cashier can just as well be your weak point.

What I'm trying to say is that knowing about the inner workings of a piece of technology does not implice you can (or will) abuse it to your or anybody else's advantage.

But this discussion is starting to become a bit off topic.

Happy cheers,

Tom

Re: Questions on GSM Penetration test

SecurityFocus Penetration: Re: Questions on GSM Penetration test

CISPP 27411

(I would have loved the number twenty four seven, four eleven :-)

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Tom Buelens: "Re: Questions on GSM Penetration test"](#)
- **Maybe in reply to:** [ricci ieong: "Questions on GSM Penetration test"](#)
- **Next in thread:** [Fernando Cardoso: "RE: Questions on GSM Penetration test"](#)
- **Next in thread:** [Emmanuel Gadaix: "Re: Questions on GSM Penetration test"](#)
- **Reply:** [Fernando Cardoso: "RE: Questions on GSM Penetration test"](#)
- **Reply:** [Wouter Slegers: "Re: Questions on GSM Penetration test"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)