File 20120124.0613: Notes from meeting with Dr Martin, via Google+ Hangout:

Dr Martin is in Singapore, at 2045 in the evening; for me it is 5am. Andrew Paverd postponed the reading group until next week, so Dr Martin and I had our own reading group and impromptu chat about the paper.

It's a little early for April Fool's day. Why did they do it? You don't provide incremental feedback during the authentication process; that's a classic security blunder. I read about this problem in high school, probably in Donn Parker's book. This was known in MULTICS if not before. It makes we wonder what other fundamental security blunders they made: is there a log file somewhere containing the wrong guesses at the PIN? It's like a classic example of how not to design a security protocol.

Not a very well written paper, according to Dr Martin. I agree with that. It lacks detail in places where it needs it, aside from the writing. But it was still tremendously interesting, because of what it shows but doesn't even say.

How many things can you find wrong with this picture? It's like an exam question on how not to do it. Dr Martin is in fact using it in his MSc class as an exam question. I hope one of his students reads the standard and finds the real reason for the design.

I thought it looked like a backward compatibility feature, to support some vendor's implementation that allows 4-digit PINs. It explains why it was designed into the protocol.

Too many features: why pushbutton *and* PIN *and* registrar PIN? Dr Martin said it smacks of three vendors, each of whom had a solution, and they combined all of them into the standard. But how did presumably smart people on the standards committee let this one by? Had they all been at the pub the previous night? WPA is secure and well-designed; how did this get layered on top?

There are just so many things wrong with this protocol: the lack of a consistent security lockout, which would have blocked the attack—interesting that the author found some routers that crashed internally, probably due to an overflow error, after too many failed authentication attempts—too many authentication options available (pushbutton, PIN, registrar PIN), the weird split-PIN verification protocol.

I've never actually used WPS; I tend not to read the instructions when I buy a new wireless router; I just hook it up and immediately go looking for the advanced setup screens to set a password, configure security, and turn off remote access. About the only things I look at the manual for are the IP address of the internal web server and a list of features I can turn off. I've never used the pushbutton, since I am usually configuring some weird FreeBSD machine with an ancient wifi card and I never ever use the Microsoft Windows setup CDs that come with it. Dr Martin has used the pushbutton method several times, since he uses a ridiculously long wifi password. I described my hex string that I use, and the fact that I have to use 128-bit WEP for compatibility with some machine in the house; Dr Martin says even 128-bit WEP can be broken in ten minutes. Whoops.

We talked about running an open wifi access point on purpose, and my setup throttling one through a transparent bridge. Don't eavesdrop on packets, although it's OK to look at the unique IP addresses for statistical purposes. I rotate through a series of SSIDs including 'LINKSYS' (to attract people looking for insecure networks to compromise), 'FREE WIFI' (to lure those incautious enough to use a network they don't know anything about) and something else intended to communicate that 'this network is provided in good faith; I don't read or mess with your traffic, use it but don't abuse it' but there is a limit to how much information you can provide in forty characters of SSID. I haven't run the experiment consistently enough or long enough to gather any meaningful data yet.

We talked about the different laws in this country and the UK about running unsecured wifi access points. On the last day of the previous government, Dr Martin noted, they got a law based on SOPA that is like a badly designed protocol in itself: unspecified conditions, lots of interactions with previous features, and once it's in production you have to support it for years and years thereafter.

I described my interaction with Security on the way out of Lockheed last week. This is my first week not working for them. I am getting work done. I want to go back to work now, to havre some results to report laster in the week.

Thanks for the email last week regarding Dr Ashbourn. It clarified a few things. Dr Martin will not go head-to-head with Dr Ashbourn unless necessary, but I don't need another person interfering.

Google+Hangout worked well. I hope it can be used next week for the Reading Group meeting. I look forward to seeing how it handles multiple channels. I reported in Dr Martin's Google+ stream that audio quality (latency, background noise, levels, compression, and reliability) is superior to Skype; video quality is grainier but seems to suffer less latency and no dropouts at all.

References