ARTICSOFT

What does 128 bit SSL encryption achieve?

Thanks to the efforts of many marketing departments to try and make things simple for users to understand, the idea has been created that only 128 bit SSL (Secure Sockets Layer) encryption is secure. Rather harder to extract from all the marketing, and rather more important, would be the information about precisely what is being secured and what contribution it makes to providing security for computer users.

SSL is used to provide an encrypted link between a point in one computer system to a point in another computer system. In some implementations it can be used to allow each of those points to check the identity of the other point. What this means is that information that flows between those two points is encrypted using a symmetric algorithm. The points in the systems identify themselves using asymmetric (or public key) cryptography.

In the case of 128 bit SSL this means that the symmetric key is 128 bits. The asymmetric or public key, used to provide identification, is generally 512 bits (not now recommended by cryptography experts) or 1024 bits. Much stronger public keys of 2048 bits could be provided but, perhaps for performance reasons, these are not in general use.

So the first thing to understand is that '128 bit' refers to the length of the cryptographic key used for encrypting information when it is passing between two points. In the case of the algorithm being used for encryption it is generally agreed that the 128 bit version is technically more resistant to attack that the 40 bit version (in this case, the more bits the better). Do note that if both ends do not have the 128 bit version they may use the 40 bit version by default. Some will tell you, others not.

So it's totally secure? Well, before rushing to say everything is secure you have to look at the system, and not just the mechanism. After all, you could say that a car is secure because it has the strongest available door locks, but maybe an immobilizer would be a good plan also!

The first thing to understand is that the information is only protected whilst passing between the two points. Outside of those, say in a database or a file on a web server, or maybe somewhere on the desktop, the information is not protected at all.

More than that, SSL doesn't know anything about the start or end point of the information it is trying to protect. If, on your computer system, you don't have a cryptographic identification key that the other end is able to recognize comes from you, then it has no idea who you are. In the same way if your system doesn't already know who the other end is then SSL doesn't help do that. Better still, some implementations don't even try to check identities.

So since from either end you don't know what you're connected to or where it is located it might be a little disingenuous to say that the system is totally secure.

Is that all? Well, not quite. Up to now we have assumed that just by having a 128 bit key the algorithm is secure. But we haven't considered how that key comes into existence. Keys are normally created using a random number generator.

Now this is fine if it is impractical for an attacker to guess (or calculate) what the key is. But if they can, then the system is nothing like as strong as it seems.

Few systems provide any reassurance on this aspect of their operation, and it is just as important as getting the algorithms right.

Also, this key is sent from one end to the other protected by the identity key (which may also have been generated). That key should be more than 512 bits if the job it is doing should be considered secure. This is similar to having a very strong front door being secured by a piece of string. The concept is right but the implementation is rather strange.

So to sum up, 128 bit SSL uses a good algorithm to securely protect information traveling between two points in computer systems. But how it has been implemented matters a lot, and what goes on around it to protect it matters a lot as well. Just because it's 128 bit doesn't mean that everything's secure.