The fallacy behind “Military Grade” or “Bank Grade” Security

“Military Grade” or “Bank Grade” encryption doesn’t mean that your information is safe.

These claims are usually more marketing than security.

Hello. My name is Michael Lester. I’m the co-founder of IronClad Family, a certified information Security Manager, Certified Information Privacy Professional, Certified Ethical Hacker, and teach ethical hacking and network security to master’s degree students at a U.S. university. I eat, breathe, sleep, and dream security!

In the next 2 minutes, I’ll give you a high-level overview of why many website claims of “Military Grade”, “Bank Grade”, or “SSL” security don’t really protect your information and what you can do about it.

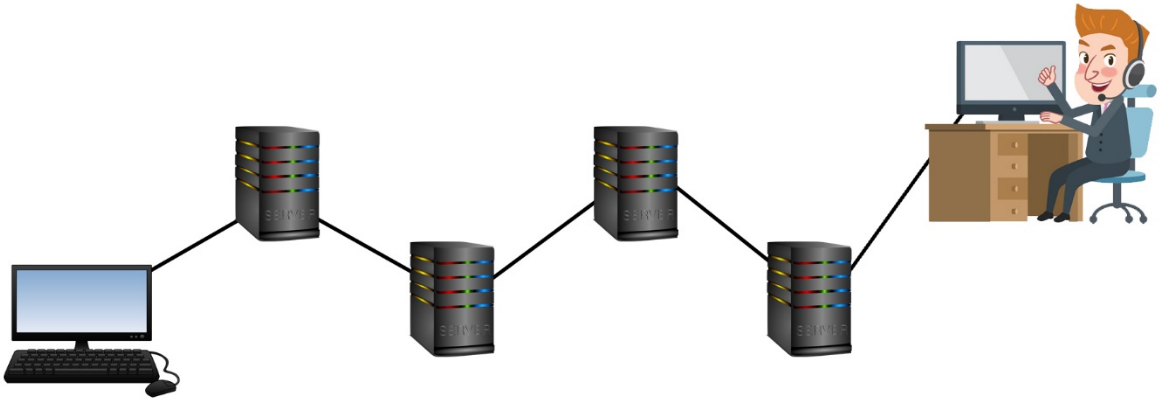
Almost every website claims to use some sort of “top level encryption.” They throw out marketing terms that sound impressive like “Bank Grade Security”, or “Military Grade Encryption”. Publishing claims like that is like a bus company saying “Our drivers are all pass a rigorous exam and are licensed.” Of course they are! If you are a bus driver, you need a driver’s license.

Here’s a little secret…If your website accepts any type of payments, then you HAVE to use a technology called “SSL” and SSL uses an encryption algorithm called AES256 which is what the military uses.

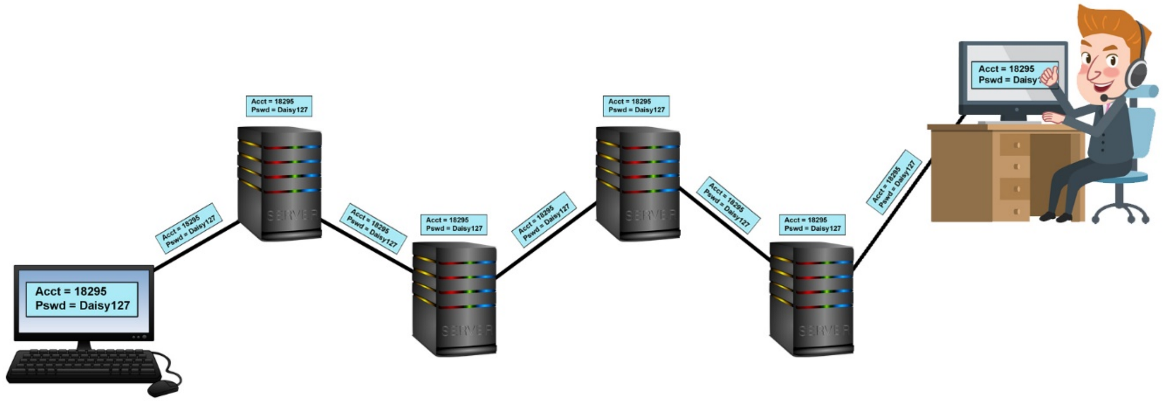
Since you can buy cookies online, “Momma’s Cookies” uses “Bank Level” encryption. So does “Aunt Martha’s Colonial Sewing Patterns” and “Chuck E. Cheese”. But let’s be serious…are you trusting your most information with Chuck E. Cheese? Protecting information entails a lot more than just using an encryption algorithm.

Let’s look at SSL. What is SSL anyway? SSL stands for “Secure Socket Layer” and is nothing more than a way to keep information confidential while it is being transmitted across the internet. Here is how it works:

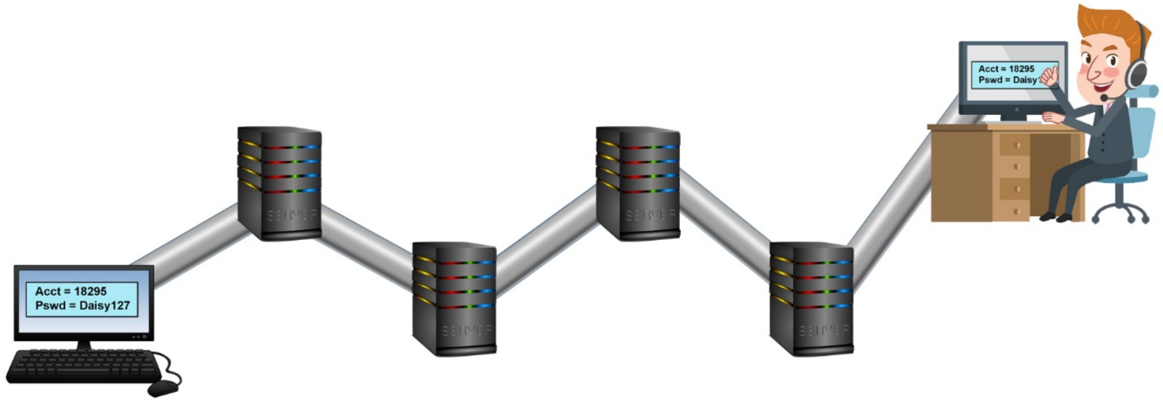
Normally when you send something from one place to another on the internet, it passes through many different computers that make up the internet and allow you to connect from one place to another.



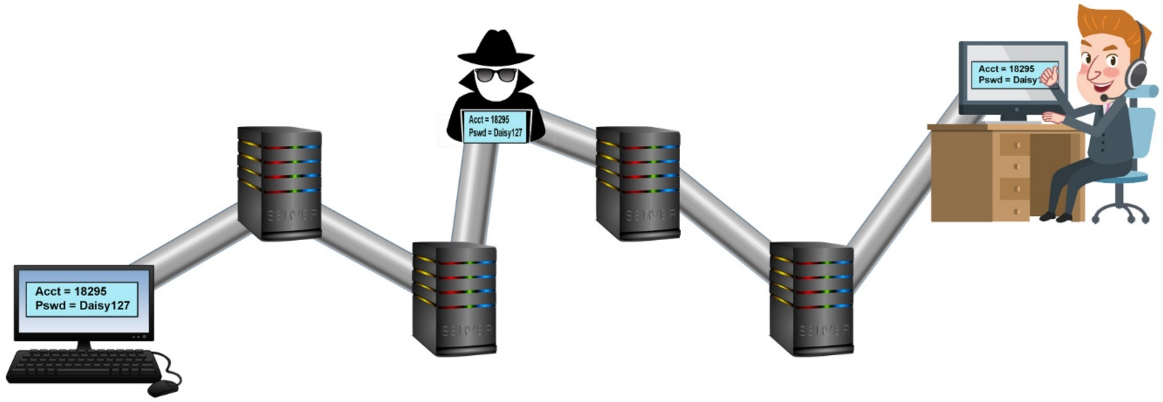
Without any kind of encryption, the information you send is readable by everyone along the entire journey your data takes through the internet.



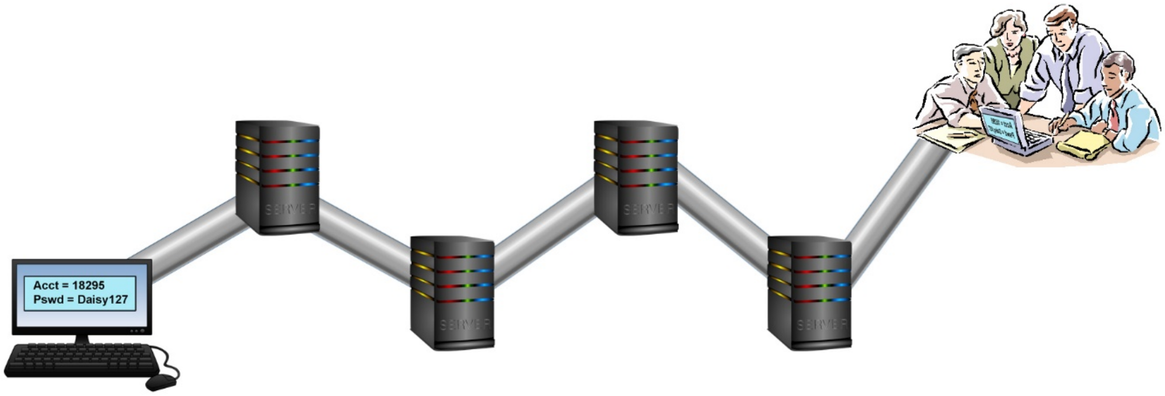
SSL (Secure Socket Layer) creates a protected tunnel from the sending computer to the receiving computer so that no one can easily read your information while it is traversing the internet. Think of it like putting a letter in an envelope before sending it through the mail. No one can see what you wrote because it is in the envelope all the way to the final recipient.



Generally speaking, this works well, but there are two major problems. The first is a hack called Man-In-The-Middle, or MITM. Using this hack, a hacker breaks the SSL tunnel and inserts themselves in the middle. They receive information, look at it or possibly change it, then send it down the tunnel again. Neither the sender or the receiver is any wiser. Using the same analogy, it is like someone opening your envelope, reading your letter, then putting it in another envelope and sending it on its way.



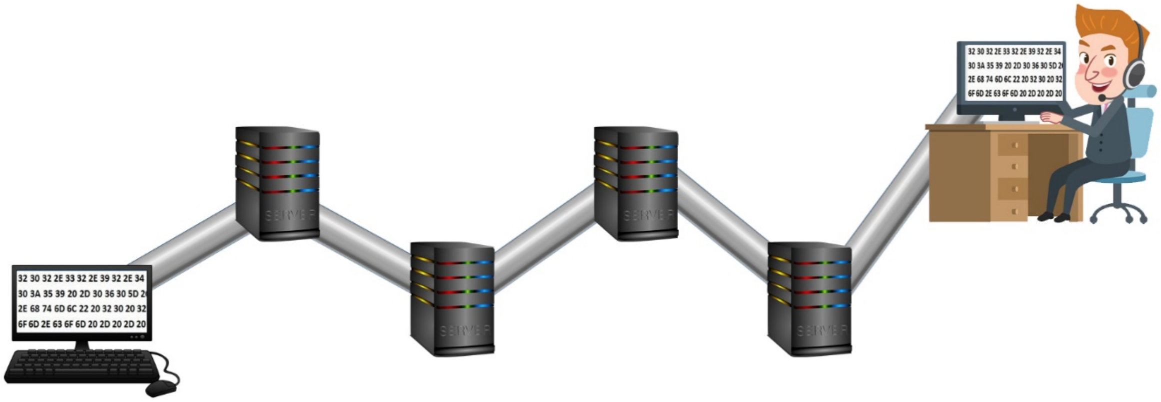
The other major problem with this is that your information might be secure from your computer to the destination computer, but once it gets there it is once again completely readable by everyone at the destination. This might make sense if you are sending instructions to a bank, because you trust the bank and want the various tellers and other employees to act on your instructions. If you are sending your information to some other company though, it means that anyone at that company can read your information.



Some companies try to address this glaring shortcoming in security by stating that they encrypt your information after receiving it. That's great, but if they are the ones that encrypted it, then they can decrypt it. That just makes sense, right? That also means that a disgruntled employee could decrypt it, or a hacker, or it could be decrypted by mistake and then released to the public. A look at any week's headlines will prove that this is A LOT more common that we'd like to believe. Encrypting your information after it is received is like locking your information in a see-through box with a lock that someone else has the keys to. Not only can others see it, but they can also unlock it at any time, and the keys can be stolen, and your information compromised.

You can see that HOW you use encryption is more important than just using encryption.

The only way to truly protect your information is with something called "Zero-Knowledge, End-to-end" encryption. Although that can sound complicated, the concept is simple. It just means that your information is encrypted on your personal computer or phone BEFORE it is sent anywhere. That means that while it is being transmitted through the internet, and after it arrives at its destination, it is already fully encrypted and no one else can see it or decrypt it because they don't have the keys! Keeping with our same analogy. It is like you putting your information in a safe, locking the safe and keeping the keys, and then sending your safe to someone else to be stored. They can't get in. Only you, or the person to whom you give your keys, can get in.


32 30 32 2E 33 32 2E 39 32 2E 34
30 3A 35 39 20 2D 30 36 30 5D 2
2E 68 74 6D 6C 22 20 32 30 20 32
6F 6D 2E 63 6F 6D 20 2D 20 2D 20
32 30 32 2E 33 32 2E 39 32 2E 34
30 3A 35 39 20 2D 30 36 30 5D 2
2E 68 74 6D 6C 22 20 32 30 20 32
6F 6D 2E 63 6F 6D 20 2D 20 2D 20

You might ask, if this is the only way to keep information safe, why doesn't everyone do that?

It's a great question. The answer is that first, although the concept is easy, implementing End-To-End Zero-Knowledge encryption is technically difficult and costly. Most companies don't want to take the time, effort, or cost and figure that you, the user or consumer, don't know any better and won't care. Second, unless you are just storing information and giving it back, it usually defeats the purpose of storing information in a way that no one can access it.

In the case of personal information vaults, however, storing your information and giving it back to your, or a designated recipient, is exactly what the service is designed to do, and therefore you should never trust any site that does not use End-To-End Zero-Knowledge encryption. Once you understand what is really happening and how secure, or not secure, your information is, why would anyone trust their important information to any company that doesn't want to take the time and effort to truly protect it. Of course, advertisers and marketers will continue to extol their company's "Bank Level Security." Luckily, now you will know what that really means.

And of course, I'd be negligent if I didn't mention that IronClad Family is the ONLY online personal information protection service that has taken the time and invested the resources to ensure that your information is completely protected using full End-To-End Zero-Knowledge encryption!