All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

All.net – Still Unencrypted for Your Protection

For some reason, many browsers these days are forcing, or very nearly forcing, all, or almost all, connections to go to https (encrypted) vs. http (unencrypted). All.net has continued to resist the forces of evil encryption infrastructure, and here is why you should too.

Encrypted is Not Secure

Influence operations, intended to help but actually maybe hurting, as usual, have caused most people using the Internet to come to believe that the little lock symbol associated with using the 'https' (encrypted – not secure) protocol makes them secure. And it worked!

- The 's' stands for 'secure' even though it should really be 'e' for 'encrypted'.
- The lock makes it seem like something is locked up
- The old definition of 'secure' was 'a feeling of safety' which influence accomplishes.

But of course, it's not true.

What about…

Integrity, accountability, use control, transparency, custody, and availability?

To understand these issues we should start by understanding what https is and does.

- HTTPS is defined in RFC 2818[1] – HTTP over TLS – which by the way discusses "Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing **secured traffic** from insecure traffic by the use of a different server port." - note the "**secured traffic**" phrase – which is correct. The "**traffic**" between two IP addresses and ports is "**secured**" (**not secure**) by encryption.
- It provides for "**secure connection closure**" per "When a valid closure alert is received, an implementation can be assured that no further data will be received on that connection." Note it does not provide for "secure" connection initiation or operation. Rather it tells us that it uses various certificate systems and such.

What it doesn't do

This list of everything it doesn't do is unlimited, for example, it doesn't wash your socks. But I will list a few relevant things it doesn't do to help you in your thinking.

- It does not assure the integrity of transmitted content.
- It does not assure availability of services or transmission, and in fact reduces it.
- It does not provide accountability for who does what.
- It does not control use or in any way prevent someone else from acting like you.
- It does not allow for detection of abuse between endpoints, but rather conceals it.

1 https://datatracker.ietf.org/doc/html/rfc2818

- It does not assure custody of content.
- It does not provide confidentiality of transmitted content.

Huh!?!?!? But what about...

I await the arguments by folks around the Internet telling me that it does do at least one of these things. They will likely tell me (and you) that it does provide confidentiality because it encrypts the traffic. And it does tend to encrypt traffic between endpoints. However:

- It does NOT protect anything at the endpoints.
- It does not prevent the use of a proxy (read machine in the middle - MITM attack).
- The traffic is subject to traffic analysis which has been shown to reveal content.
- Protocol issues can cause the encryption to be very weak or nil

And this is just the beginning…

Forcing people to use it

But that's not really what this article is about. This article is about all.net – the Web site that hosts this content, being **unencrypted**. And about the attempts to try to force us to encrypt and you to have difficulty reading our content. I consider it tortuous interference, but I have not (yet) gone to the courts to try to enforce it.

For your protection

To keep you safe from the misimpression that the all.net site provides any sort of **custody**, **confidentiality**, **use control**, or **accountability**, we have not allowed the https protocol to operate on our site. That's right! We **DO NOT PROVIDE THOSE THINGS**.

My single objective for the all.net site is to provide open access to content I decide to place there. That does not mean I guarantee you anything about it, and it does not mean I grant you the right to do anything with it other than to read/use it in your browser.

I do not guarantee in any way that I will not take any information you provide to the site and do anything I want with it. If you don't want me to have it, don't send it to me!

I do not guarantee it is pure or true or right or free from corrupt content, errors, omissions, malicious code, lies, scams, or anything else. I will tell you that I do what I can to be honest as a general rule, and try to have integrity in my life. But I have no control over anything or anyone other than myself.

And you should know

That this is true of almost every other site out there. They do not use SSL for your protection. They may use it for their protection. Or maybe they use it because of peer pressure. Or maybe they think it provides some sort of security. Or maybe they think it fools you into thinking you are safer with them. But really, the major effects are increased use of resources and payment to the encryption industrial complex.

Conclusions

All.net is and will remain unencrypted – for your protection. And if you cannot read this article because the encryption industrial complex wants to block you… tell them to stop it.

