



eSubnet Fragment Article

Beyond the Lock

A few months ago I wrote an article on how to build your own certificate authority. Certificates are primarily used for two purposes identity management and encrypted transport. The most well known occurrence of certificate usage is online shopping and banking. In both instances, the little lock in the browser has gained the reputation for providing a safe environment. VeriSign, the leader in the public certificate community states, "VeriSign secures over one million Web servers worldwide with strong encryption and rigorous authentication"

Certificates only provide protection for a portion of the chain required to complete the transaction. Now most of you reading this bank and shop online. Are you distressed to find out that the little lock has been perhaps misleading you? The lock does not lie; you just have to understand what the lock is assuring you of. The lock tells you that you can trust that you are talking to the server you think you are talking to, and that other people trust it as well. What it is not telling you, is the network you are talking over or whether the server you are talking to is trustworthy. Notice that I have not even touched on the computer local to you (another can of worms that we won't go into here).

This insecurity is important for system administrators to understand. When setting up systems which require end-to-end on the wire encryption, you have to keep in mind devices such as load balancers, and SSL accelerators. Is the encryption only required up to the network edge or should it penetrate deeper than that, and if so, do the same rules need to apply? Before you begin deployment, questions like these should be considered thoroughly.

Design specifications for systems are vital to both management and the IT department. Management needs to know that IT will deploy a system which covers any and all concerns that management is aware of; and likewise, IT needs to know what management is looking for so they may deploy the correct system so that it immediately functions as desired.

I mentioned the end user local computer, an area of potential calamity. The computers found within your sphere of influence you can make certain assurances, control over download and installations policies, anti-virus updates, spam and spyware, all can be filtered and/or automated at the network edge. The system administration team has control over the works.

In recent months, there has been a push in general IT media for products and means which enable, and seemingly encourage, mobile users and remote access to resources. Many of eSubnet's clients are looking at ways to extend the employee work day by providing easier access to network resources.

This extended 'always able to work' access comes at a cost. The cost is real, and quantifiable if you are looking to do things correctly. The main issue is the end users home computer. A case in point, an organization spends X number of dollars putting in place firewalls, filters and scanners to protect Y number of computers. This protection is in place to protect the intellectual property of the organization. Then, remote access is enabled and typically X and Y are not incremented. The value of the protection investment is not merely diminished by $X/(X+1)$ but is potentially changed to zero due to a single key-logger unknowingly downloaded by someone else who has access to the home computer platform.

What happened is the access to resources has stepped outside of the system administrator's sphere of influence. Not necessarily a good move if privacy and security are among your goals. One should not discount the importance of encrypting sensitive traffic traversing the public Internet but also keep in mind the many avenues by which data leakage can occur. When considering remote access, ask yourself, "Is the change in the risk profile worth the 'always able to work' benefit?"

Originally published January, 2009

Republished: February 2009 in [TLOMA](#) Today

About the Author

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at <http://www.esubnet.com/fragment.html>.

Reprints

1. Commercial use: Commercial newspapers, magazines and websites that wish to reprint an article should contact eSubnet for permission.
2. Non-Commercial use: Any reproduction of content (excerpt or full text) by nonprofit organizations or companies wishing to share information with their members or clients requires that you notify us, whether for print or online usage.

Regarding reprints, contact Mr. Danielli at [rdanielli\(at\)esubnet.com](mailto:rdanielli@esubnet.com) or at (416) 203-1223.