What E-Commerce Really Needs

.Introduction

E-Commerce refers to the conduct of commerce through electronic systems. This means, for example, buying and selling merchandise through an electronic system. Popular e-commerce includes individuals using their personal computers (PCs) connected to the Internet to make purchases from online stores.

Much popular e-commerce uses Public Key - Private Key (Asymmetric) Encryption, or a combination of Public Key - Private Key (Asymmetric) Encryption and User ID/User Password.

.Existence Of Risks

Risks to the security of Asymmetric Encryption have been discussed in previous papers.

- The strength of the Public Keys that the Client (the User and his/her computer) and the Server (the web site with whom the User is transacting business) is crucial to the entire process. If it is not sufficient, the entire ensuing transaction could be compromised.
- The need for the Client (User) to know, "with whom am I transacting?" typically requires a trusted third party. The arena of trust thereby grows, and there is no central "authority" that gives these third parties their "trust".
- User ID/Password are traditionally considered a whitewash of security unless the Passwords are well chosen.

.Why this Happened

Certain trailer hitches are made specifically for passenger cars. They allow motorists to pull trailers without the need to purchase a tractor or truck. In general, this is a bad idea unless the motorist is pulling a small trailer. The transmission, trans-axle, engine and brakes could be placed under undue stress and subjected to overheating. They can be damaged and this situation can also result in unsafe motoring. Nevertheless, companies manufacture such hitches and motorists purchase them and use them.

In the pursuit of e-commerce, designers have defaulted to the "Web". Specifically this refers-to:

- HTTP (Hyper Text Transfer Protocol)
- HTML (Hyper Text Markup Language)
- Web pages
- Web servers such as Apache and IIS
- Web Browsers such as Internet Explorer and Navigator

In addition, the architectural approach is to allow users to conduct so-called secure e-commerce without the need for previously agreed-upon and previously conveyed encryption keys.

The risks mentioned above and the problems identified in previous papers are the natural and expected result of all of this.

.An Alternative

A custom client-server application program can and should be developed to allow the e-commerce process to be conducted entirely under the wraps of Symmetric encryption.

This means that the server would not be running an application such Apache or IIS and the client would not be running an application such as Internet Explorer or Navigator.

This approach would require previously agreed-upon and previously conveyed encryption keys. The traditional mail system is an obvious candidate. This should not be a problem since the banking industry has shown us that this model works quite well. Specifically:

- Credit cards come **in the mail**
- If you lose one or it is compromised, the new one comes **through the mail**
- ATM cards come **through the mail**
- ATM PINs come **through the mail**

The use of a mailed encryption key in a Symmetric Encryption, client-server, e-commerce application program would ensure:

- secure transactions
- user authentication
- server authentication
- non-repudiation