The Unspoken Risk of E-Commerce

.Introduction

Previous papers have discussed some of the weak points of current e-commerce systems that use Public Key - Private Key (Asymmetric) Encryption. These presentations address the situation of an authorized user attempting to gain access to a specific user's account.

This paper addresses the security/risk-of-compromise of the server database as a whole.

.Damage Equation

..One-On-One

If an unauthorized user gains access to a specific user's accounts, it is a one-on-one situation. Whether we are speaking about the unauthorized user being able to place orders using another person's account or an unauthorized person gaining access to another individual's banking data. it is a one-on-one situation.

While the damage that could be done is serious, particularly to the individual whose security has been breached, in the "damage equation", the clean-up and restoration is relatively small.

..One-On-Many

If an unauthorized user gains access to an entire database, such as 100,000 credit card numbers, it is a one-on-many situation.

The damage that could be done is not just serious. It is huge. In the "damage equation", the clean-up and restoration could be monumental. In addition, the reputation of the organization that was compromised could be seriously hurt.

.An Approach

This paper does not suggest that the solution to this problem is simple, but it might be.
If:

- the entire database of, say, credit card numbers were encrypted with Symmetric encryption, using a program such as KetuFile, and
- the server only decrypted the numbers as they were needed,
- the server then destroyed the un-encrypted version of the credit card number after it was no longer needed,

then it could be possible to substantially thwart the attempts of an unauthorized user from inflicting a compromise that was a major event.