The Zen of Information Security

Joshua Hill
March 1st, 1999

The Goals of Information Security

Aside from Fame, Fortune and the Pursuit of Members of the Appropriate Sex

What is Information Security?

1. Information Integrity
    - Persistence of data.
    - Ability to access data.
    - Immutability of static data
    - Verifiability of data consistency

2. Confidentiality
    - Ability to control access to your data
    - Ability to securely transfer your data between trusted sites

3. Authentication
    - Data Authentication
    - Entity identification

4. Non-Repudiation.

Information Integrity

The Great Information Taco

Least ‘Sexy’ of the Information Security goals.

Persistence of information
Accomplished with

- Backups
- RAID
- Mirroring
- Eternity servers
- Data Havens

Can conflict with the goal of **confidentiality**.

Verification of data
Accomplished by:

- cryptographic hashes
- MACs
- signatures.

Confidentiality

The Obfuscated Burrito

The most widely recognized Information Security goal.

Accomplished with

- Envelopes
- Safes
- Briefcases attached to very large men named ‘Butch’.
- Encryption

Can conflict with the goal of **Information Integrity**.

Authentication:

The Chili Rieno of Love

One of the most valuable information security goals.

Includes:

1. Verification of data authenticity
2. Verification of entity identity.

Accomplished with

- Signatures
- Seals
- Digital Signatures
- MACs
- Shared secret encryption

Shares verification goals with **Information Integrity**.

Non-Repudiation:

The Misunderstood Enchilada

The most commonly neglected and misunderstood goal

Accomplished with

- Public Notary and Witnesses
- Digital Signatures

Shared Secrets don't work.

Required for

- Legally binding contracts
- Electronic commerce

This goal is related to **Authentication**.

The Foundations of Information Security

The Method to the Madness

Trust and trust Management

- Implicit and Explicit assignments of trust
  - Buying a carton of milk from the store
  - Driving on the freeway

Information Security transfers trust:

- Trust in the machine
- Trust in the data
- Trust in identity of another

At it's **very** best, Information Security can provide the same trust as in the real world.

Further Foundations to Information Security

Further Madness

How do they do that?

1. **Minimize** secret information.
   - The meaning of 'Security through Obscurity'
   - The principle of information leverage.

1. Use well developed protocols.
   - Try to use pre-developed protocols
   - Peer Review of original protocols

1. Rely on understood primitives.
   - **NEVER** make your own primitive.
   - **NEVER** use new or poorly understood primitives.
   - If it sounds too good to be true, it is.

The Truth is Out There!

Trust no one!

I wasn’t

wrong,

I was

lying.