**Naming**

In practice, many successful naming systems have been designed. For example:

1. The Internet Domain Name Systems that primarily map hostnames to an IP address. For example, kitcampus.com has the IP address 212.206.211.148. For more details, see: http://www.ietf.org/rfc/rfc1034.txt
2. The IETF Uniform Resource Identifiers (URI). For example, the URL object http://www.ietf.org/rfc/rfc2396.txt contains the generic syntax for URL
3. The Abstract Syntax Notation version 1 (ASN.1) naming system for objects. For example, when Microsoft designs a new file format for a new software product, in the Object Identifier Tree, it will be registered as 1 2 840 113556 4 xxx, where 1 means ISO, 2 means ISO-Member-countries, 840 means USA, 113556 means Microsoft, and xxx means Microsoft new file format.
4. CORBA naming systems. For example, see http://www.cs.tcd.ie/Greg.Biegel/nds106/CORBA.html.
5. Java Naming conventions. For example, a well-named Java package could have a name com.sun.javax.swing.kitsecurity.

Naming systems have been one of the hottest attacking points. Indeed some Trojan Horses use naming conventions to attack the system (e.g., some attacks on DNS).

**Passwords**

Federal Information Processing Standards Publication 112 (FIPS 112): The Standard for Password Usage (http://www.itl.nist.gov/fipspubs/fip112.htm), 1985.

Want to know how insecure are the password systems for most Windows applications? Check http://www.pwcrack.com/

Password crackers: http://www.password-crackers.com/

http://www.atstake.com/products/lc/index.html

An analysis of weakness in Microsoft PPTP password hashing: http://www.counterpane.com/pptp.html

RSA Secure ID is a hardware token which displays the owner's current password and is generally only valid for one minute. For more details check http://www.rsasecurity.com/

In recent years, password authenticated key exchange protocols have been designed to defeat off-line dictionary attacks - even if the password is chosen from a small sample space. The most important protocols

include Encrypted Key Exchange (EKE) from AT&T, SPEKE from Phoenix and SRP from Stanford University (SRP is also a protocol for Internet applications standardized by IETF). Password authentication-based key exchange protocols are currently being standardized by the IEEE 1363 working group. See http://grouper.ieee.org/groups/1363/index.html for more details.

**Access Control**

D.E.R.Denning. *Cryptography and Data Security.* Addison-Wesley Publishing Company. ISBN O-201-10150-5, 1982.