AGENDA

Computer image verification & Authentication

Special needs of evidential authentication

- It may be possible to seize the computer system, this risks violating the basic principle *innocent until proven guilty* , by depriving an innocent party his or her use of the system

It should be perfectly possible to copy all details of the computer in the manner that leaves the original system untouched and yet makes data available for forensics analysis

- The court needs evidence that the evidence has been protected from accidental or deliberate modification it is not the

Special needs of evidential authentication

- The protection takes two forms
- *A secure method of determing that the data has not been altered by even a single bit after the data is copied*
- *A secure method of determing that the copy is genuinely the one taken at the time and on the computer in question*
- ***This is collectively called digital image verification and Authentication protocol***

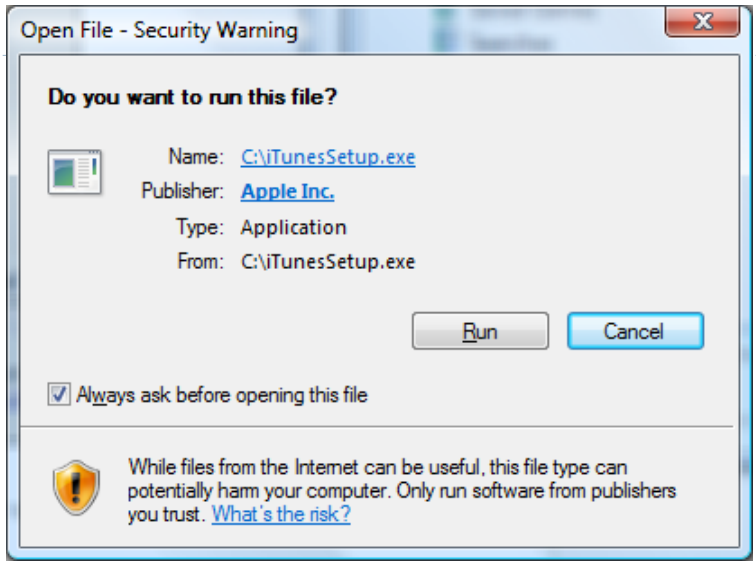
Digital IDs & Authentication Technology

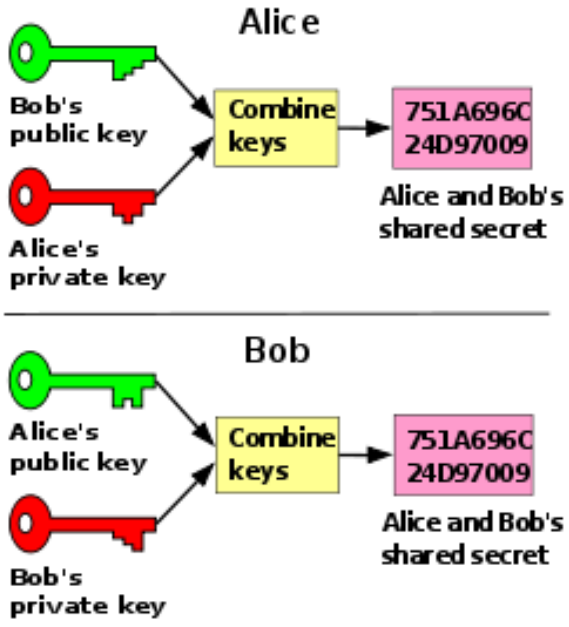
Authenticode

- Microsoft Authenticode allows developers to include information about themselves and their code with their programs through the use of digital signatures.
- Through *Authenticode,* the user is informed:
  1. Of the true identity of the publisher
  2. Of a place to find out more about the control
  3. The authenticity of the preceding information
- Users can choose to trust all subsequent downloads of software from the same publisher and all software published by commercial publishers that has been verified by VeriSign.

Public Key Cryptography

- In public key cryptographic systems, every entity has two complementary keys (a public key and private key) that function only when they are held together.
- Public keys are widely distributed to users, whereas private keys are kept safe and only used by their owner.
- Any code digitally signed with the publisher's private key can only be successfully verified using the complementary public key.
- Code that successfully verified using the publisher's public key, could only have been digitally signed using the publisher's private key, and has not been tampered with.


Open File - Security Warning
Do you want to run this file?
Name: C:\iTunesSetup.exe
Publisher: Apple Inc.
Type: Application
From: C:\iTunesSetup.exe
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?


Alice
Bob's public key
Alice's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's public key
Bob's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret

Digital IDs & Authentication Technology

Certificate Authorities

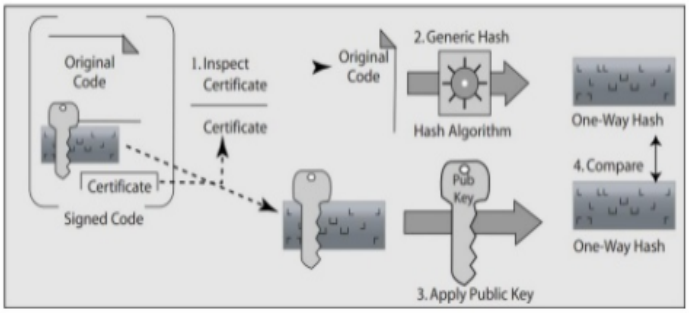
- Certification Authorities such as VeriSign are organizations that issue digital certificates to applicants whose identity they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.
- VeriSign has the following responsibilities:
  1. Publishing the criteria for granting, revoking, and managing certificates
  2. Granting certificates to applications who meet the published criteria
  3. Managing certificates
  4. Storing VeriSign's root keys in an exceptionally secure manner
  5. Verifying evidence submitted by applicants
  6. Providing tools for enrollment
  7. Accepting the liability associated with these responsibilities

Digital IDs & Authentication Technology

Digital ID

- A Digital ID/Certificate is a form of electronic credentials for the Internet.
- A Digital ID is issued by a trusted third party to establish the identity of the ID holder.
- The third party who issues certificates is known as a Certificate Authority (CA).
- Digital ID technology is based on the theory of public key cryptography.
- The purpose of a Digital ID is to reliably link a public/private key pair with its owner.
- When a CA such as VeriSign issues a Digital IDs, it verifies that the owner is not claiming a false identity.
- When a CA issues you a digital certificate, it puts its name behind the statement that you are the rightful owner of your public/private key pair.

How Authenticode works with VeriSign Digital IDs?



Authenticode: VeriSign Digital ID process

1. Publisher obtains a Software Developer Digital ID from VeriSign
2. Publisher creates code
3. Using the SIGNCODE.EXE utility, the publisher
    - Creates a hash of the code, using an algorithm such as MD5 or SHA
    - Encrypts the has using his/her private key
    - Creates a package containing the code, the encrypted hash, and the publisher's certificate

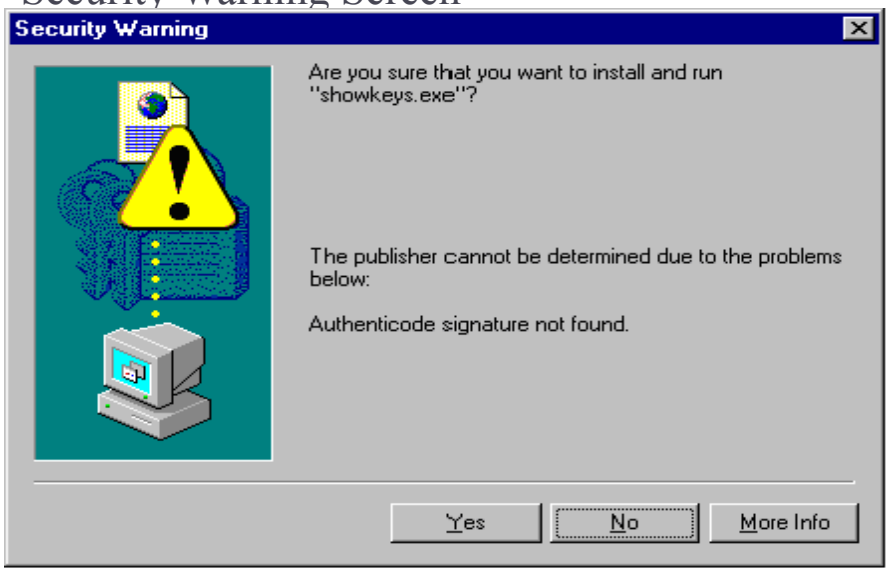
How Authenticode works in Verisign

4. The end user encounters the package
5. The end user's browser examines the publisher's Digital ID. Using the VeriSign root Public Key, which is already embedded in Authenticode enabled applications, the end user browser verifies the authenticity of Software Developer Digital ID (which is itself signed by the VeriSign root Private Key)
6. Using the publisher's public key contained within the publisher's Digital ID, the end user browser decrypts the signed hash.
7. The end browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
8. The end user browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has the confidence that the code was signed by the publisher identified in the Digital ID, and the code hasn't been altered since it was signed.

Time stamping

- When you sign code , a hash of you code is send to VeriSign to be time stamped.
- As a result when your code is downloaded , clients will be able to distinguish between code signed with an expired certificate.

Security Warning Screen



2. Practical Consideration

- It is useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected.
- Other forensic experts may argue against some or all of them:
    1. Forensic data collection should be complete and non-software specific, thus avoiding software traps and hidden partitioning.
    2. In operation, it should be as quick and as simple as possible to avoid error or delay.
    3. It should be possible for anyone to use a forensic data collection system with the minimum amount of training.
    4. Necessary costs and resources should be kept to a minimum.
- To meet the conditions specified in items 2, 3, and 4, the digital integrity verification and authentication protocol must be tailored to suit.
- Only investigators issued with a valid digital signature would be able to complete copies.

3. Practical Implementation....

- A minimum amount of reliance is placed on the technical ability of the operator/investigator.
- It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary.
- It must also be understood that procedures are implemented to verify that information is copied correctly.
- This information is stored on each cartridge within a copy series.
- Also stored on each cartridge is a reference area containing copy-specific information such as CPU type and speed, hardware equipment indicators, copying drive serial number, cartridge sequence number, exhibit details and reference comments, operator name together with a unique password, and the real date and time as entered by the operator.
- The cartridge is divided into blocks of an arbitrary chosen size. Blocks may contain reference, ROM, CMOS, or disk data depending on their location on the cartridge. Each cartridge contains the information copied from the suspect drive on a sector by sector basis.

Security Considerations

- Computer forensics investigators are constantly discovering new vulnerabilities in old image verification and authentication products.
- As a result CIOs (Chief information Officers) are devoting more money and time to image verification and authentication security.
- Staff-members are the ones who make sure viruses don't come in and holes aren't created in the firewall.
- They have to understand that most business is built on trust, and their role in maintaining trust is crucial.
- It's difficult, perhaps impossible, to measure the return on investment in security.
- You have to protect your data. It only takes one time –-one hacker getting in and hacking all your financial data.
- It would be irresponsible on CIO's part not have the toughest image verification and authentication security possible.