



Microsoft Authenticode for the Small Independent Software Vendor

By Richard Marsden

<http://www.winwaed.com>

This presentation is being submitted in partial fulfillment of the requirements for

MGT 5387 Foundations in Information Assurance, Spring 2006.
Graduate School of Management, University of Dallas

Submitted to Prof. Branden R. Williams, 20th March 2006



Overview

- Microsoft's Authenticode® Code Signing Technology
- Small independent software vendors (Micro ISVs)
 - Prime delivery channel: Internet download
 - General reluctance to use Authenticode
- Survey of Micro-ISV attitudes to Authenticode

This report and presentation look at Microsoft's Authenticode code signing technology from the point of view of small independent software vendors (micro ISVs). Although these vendors should benefit from the verification of authenticity that Authenticode aims to provide, many micro-ISVs are reluctant to use Authenticode. This report also includes a survey of micro-ISV attitudes towards Authenticode, analyzing any perceived deficiencies – real or otherwise.



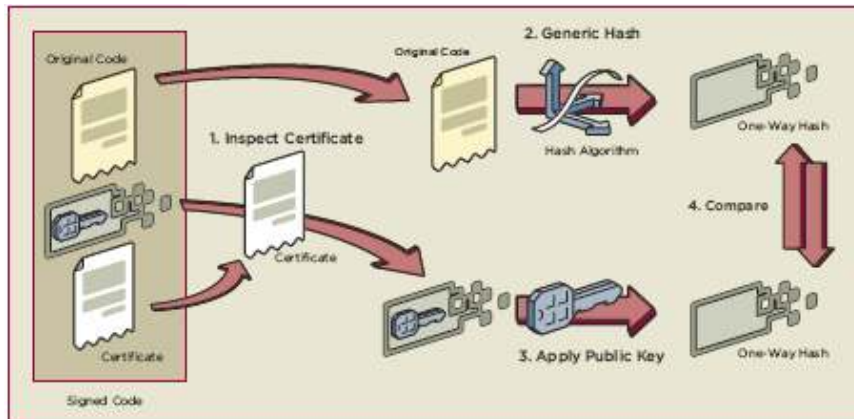
Microsoft Authenticode

- Microsoft release ActiveX technology
 - Downloadable COM objects
 - Have wide range of abilities
 - Significant security risk
- Authenticode introduced in 1996
 - Signs Windows executable code using a digital certificate
 - Certificates issued by a Certification Authority (CA)
 - Demonstrates software has not been tampered with
 - Authenticates who the publisher is
 - Signed malicious code can then be acted upon by law enforcement, or by certificate revocation.

During the mid-1990s, Microsoft release their COM object technology in a downloadable form and named it “ActiveX”. ActiveX was intended to add the ability to use “smart controls” in web pages. However, it was quickly demonstrated that ActiveX had a wide range of abilities and could take control of a user’s machine. This was demonstrated by Fred McLain’s Internet Exploder demonstration ActiveX control (<http://www.halcyon.com/mclain/ActiveX>).

Microsoft’s answer was to introduce its Authenticode code signing technology in 1996. Authenticode allows a publisher to sign their software – eg. ActiveX control .exe executable using a digital certificate. This allows the end user to determine the publisher’s identity and whether the software has been tampered with since it was signed. Digital certificates are issued by an approved Certification Authority. As a publisher must prove their identity to the Certification Authority, so it should be able possible to identify the real-world publisher of malicious signed code.

Using Authenticode



VeriSign (2005). "VeriSign Code Signing for Microsoft Authenticode Technology" <http://www.verisign.com/static/030999.pdf>

A publisher obtains their digital certificate from the Certification Authority (CA), with matching public and private keys.

The slide illustrates how the publisher signs a piece of software using this certificate. An executable is signed with Microsoft's SIGNCODE.EXE utility. This creates a hash (typically SHA1 but MD5 is also supported) of the certificate information and executable. The hash is then encrypted using the private key and included as a part of the executable file along with the public key. When the end user receives the executable, the encrypted hash is decrypted using the public key. A new hash is created from the executable. The certificate is valid if the two hashes are identical, and the certificate has not expired.

Certificates are supported by a Public Key Infrastructure (PKI) hierarchy. Windows ships with many approved CA certificates. Publishers also have the option of including the CA's own certificate to cover situations where a new CA's certificates have not yet been fully deployed on end user machines.

Warnings from Unsigned Code



Authenticode is available for all versions of Windows since Windows 1995, and it has shipped with all recent versions of Windows. However, it is only with Windows XP Service Pack 2, that Authenticode has been switched on as default. This is an example of the warning dialog box that Windows XP displays if an attempt is made to run an unsigned executable that has been downloaded from the Internet.

This has been described as a 'scary' dialog box by many Micro-ISVs, and was the direct cause for the author to use Authenticode to sign his own downloadable products.



Authenticode Weaknesses: Publisher Verification

- CAs must verify that a certificate applicant is who they claim they are
 - Must reject fraudulent applicants
 - Commercial need to make it easy for bona fide applicants
- Fraud
 - VeriSign issued two certificates to “Microsoft Corporation” in 2001.

CAs walk a fine line when verifying applications for new digital certificates. They must try to avoid issuing certificates to fraudulent applicants, but for commercial reasons they must also make it easy to obtain certificates.

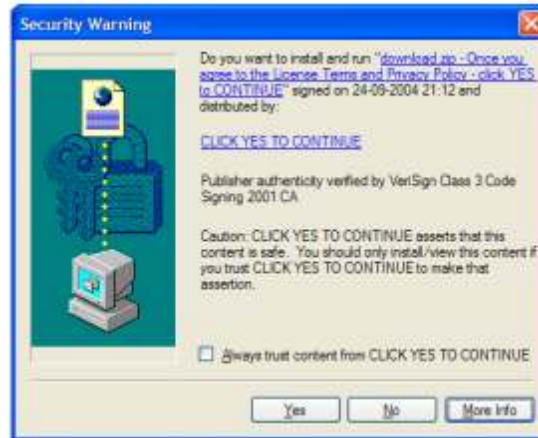
CA requirements vary widely and typically require some form of business license. Comodo (<http://www.instantssl.com/code-signing/index.html>) have been known to accept a DBA certificate signed by a County Clerk, and a cancelled check. County Clerks do not check for trademark infringement and banks usually only require a DBA certificate to open an account. Therefore it is relatively easy to obtain a fraudulent certificate for a lesser-known 3rd party.

If you thought that this would not happen for a well known third party such as “Microsoft”, and a better known CA such as VeriSign, think again!

In a well publicized case, VeriSign issued two Authenticode certificates in 2001 to someone fraudulently posing as a Microsoft employee.

Although the bogus certificates could be identified by their date, this was very embarrassing for both Microsoft and VeriSign.

Authenticode: Fraud Example



[1] Charles Sinclair (ResultsWare Limited) personal communication (March 2006)

Here is another example of a fraudulent certificate issued by VeriSign, communicated to the author by Charles Sinclair of ResultsWare Limited. Sinclair found this example whilst investigating a pirate copies of his own software, on a known pirate software (“warez”) site.

VeriSign managed to approve a certificate to “CLICK YES TO CONTINUE”. The alternative is that the certificates can be hacked – something that Microsoft claim is virtually impossible.



Other Weaknesses

- Faulty implementation
 - Previous bugs have caused Authenticode to fail and execute unsigned code without confirming with the user
- A liability-limitation tactic?
 - Microsoft might claim no liability if it could show that the user ran unsigned code.

Although relatively rare, Authenticode has been subjected to the occasional bug. The most significant (MS Security Bulletin MS01-017) resulted in unsigned code being executed without confirmation from the user, under certain specific conditions.

Another perceived weakness when it was introduced was put forward by Mark Seecof (Risks Digest Volume 18, Issue 89, 1997

<http://catless.ncl.ac.uk/Risks/18.89.html#subj12>). Seecof argued that Authenticode was a liability-limitation exercise by Microsoft. If a user with a non-functioning Windows system had previously executed unsigned code, then Microsoft would be able to avoid responsibility.

Nine years later, Microsoft have not taken this tactic.



Micro-ISVs

- Independent software vendors with 1-2 people
- Significant since the introduction of personal computers
- Primary Distribution channels:
 - Shareware during the 1980s and early 1990s
 - Downloads from websites for the last 10 years
 - Rely on trust from their potential customers
- Often reluctant to use Authenticode
 - Why?
 - Survey

“Micro-ISV” is a relatively new term, but it refers to a segment of the software industry that has been significant since the advent of the personal computer, namely very small (1-2 person) independent software vendors who write and sell their own software.

In the past ten years, micro-ISVs have moved to Internet downloads as their primary distribution channel for their products. With the increasing number of viruses, worms, spy-ware, and other malicious downloads, micro-ISVs have to rely on the trust of their potential customers. This trust directly translates into increased downloads and sales.

One would expect that micro-ISVs would embrace Authenticode as a means to verify their bona fide status, however take-up has been relatively poor. A survey was conducted to analyze reasons for this poor take up, and whether there were any perceived deficiencies in Authenticode.



Survey Results: Summary

- 41 respondents
- 90% in US, Canada, or Europe
- 82.9% from 1-2 employee vendors
- 92.7% develop for Windows
- 97.6% offer software for download
- 95.1% have heard of Authenticode before
- 34.1% currently use Authenticode

The next few slides illustrate some of the main results from the survey. The report plots all results and discusses them in more detail.

Survey details were posted to a number of forums and newsgroups aimed at micro-ISV / shareware authors; and 41 completed questionnaires were received. Reflecting the target forums, 90% were from US, Canada, and Europe. No responses were received from Africa or South America.

The survey was successful at targeting the required audience of 1-2 person operations who sold Windows software for download off the Internet.

The premise of this report was also quantified by the result that 95.1% of respondents had heard of Authenticode, but only 34.1% were actually using it.



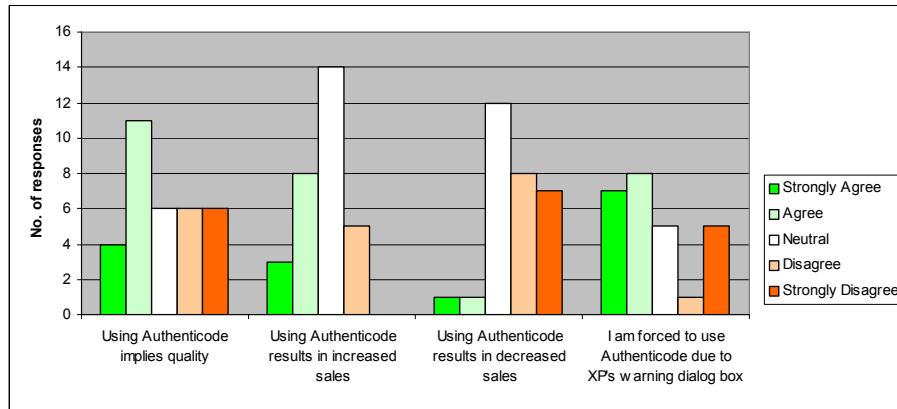
Survey Results: Problems

- 53.6% reported no problems with Authenticode
- 25% Found it was difficult to find information about using Authenticode
- No one reported software instabilities due to Authenticode
- Other responses included:
 - *"Too much effort, costly, and not allowed"*
 - *"Tools are rudimentary"*
 - *"Haven't found a way to integrate it"*

One possible reason for a low take-up rate is that micro-ISVs have experienced problems with Authenticode.

The most significant problem reported was that 25% of respondents found it difficult to find information about how to use Authenticode. Write-in responses included two referring to usability.

Results: Statements



Respondents were asked if they agreed or disagreed with a variety of statements.

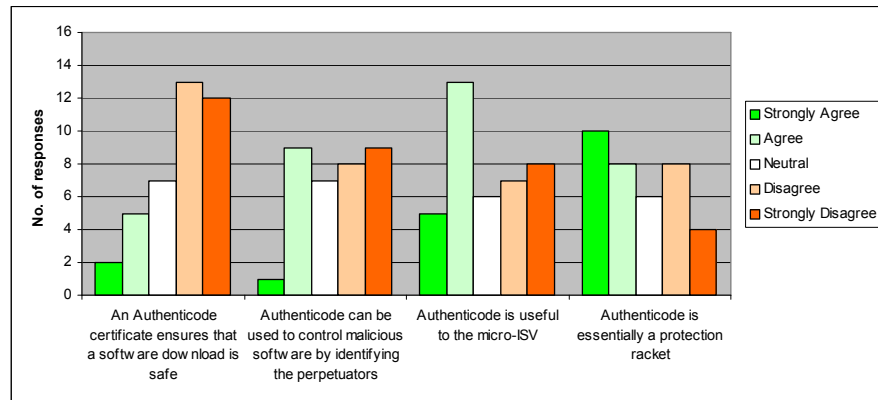
There was a mixed response that the use of Authenticode implies quality.

Respondents strongly disagreed with the statement that Authenticode could lead to a decrease in sales.

Although there was a similar agreement that its use results increased sales, a sizeable minority disagreed with this assertion.

Many agreed that XP's warning dialog box forced them to use Authenticode.

Results: Statements



Respondents correctly disagreed with the statement that Authenticode ensures that a download is a safe. There was a similarly correct, strong agreement to the statement that Authenticode verifies program authenticity (not shown here but included in the report).

However, most respondents disagreed with Microsoft's claim that Authenticode is intended to identify a publisher of malicious software.

Many thought that Authenticode was moderately useful to the micro-ISV, although there was a significant tail of those who strongly disagreed that it was useful.

There was a fairly even response to the statement that "Authenticode is essentially a protection racket", although this was biased towards agreement. This statement was included because the author has seen it stated before. This is because a publisher has to pay a CA in order to remove the warning dialog box. A number of vocal agreements with this statement were received in the write-in section of the questionnaire (see Appendix 2 of the report).

Further statements not plotted on these slides asked about public understanding, and cost. A very strong agreement was received (34 agree or strongly agree) to the statement that Authenticode certificates are poorly understood by the general public. Clearly Microsoft and the CAs need to educate the general public about the warning dialog boxes.

Not surprisingly, no one thought that certificates were too cheap, but many thought they were too expensive. A very neutral response was received to the statement that "Certificates are too easy to obtain".



Conclusions

- Micro-ISVs need to demonstrate bona fide nature of their software to increase sales
- Authenticode is currently the best way to do this
- Need better education from Microsoft and the CAs
 - Many Micro-ISVs find it difficult to find information
 - The general public is thought to have a poor understanding of the resulting warning dialog boxes
- Fraudulent certificates are a problem
 - Microsoft and/or the CAs must actively follow up on fraudulent certificates
 - Prosecutions
 - Certification Revocation
 - Demonstrate that Authenticode really does work

The survey results are discussed in further depth in the report, but a number of conclusions were reached.

Authenticode should help to demonstrate bona fide nature of Micro-ISV software, and Authenticode currently appears to be the best way to do this. However despite a high awareness amongst Micro-ISVs, take-up is low.

Education and information were both perceived as a problem. 25% of Micro-ISVs reported problems finding information about how to use Authenticode. It was widely considered that the general public had a very poor understanding of the resulting dialog boxes and what they meant.

Fraudulent certificates are also a problem. This is discussed in further detail in the report, but it is unclear if Authenticode actually works in a way that Microsoft claims it is intended. There an almost complete lack of reports of certificates being revoked, or prosecutions occurring.

The earlier example of “CLICK HERE TO CONTINUE” was reported to VeriSign in a written letter, but VeriSign never replied. Write-in comments also echoed the view that there would be a greater faith in Authenticode if there were visible signs of certificates being revoked or prosecutions occurring.

Such actions would also demonstrate that Authenticode is not a protection racket.



Selected Bibliography

- Atkinson, Bob (1997, March). "Comments and corrections regarding Authenticode" . The Risks Digest v18, Issue 85. Available: <http://catless.ncl.ac.uk/Risks/18.85.html>
- CERT (2000). "Results of the Security in ActiveX Workshop Pittsburgh, Pennsylvania USA August 22-23". CERT® Coordination Center. Available: http://www.cert.org/reports/activex_report.pdf
- Grimes, Roger (1996). "Authenticode". Microsoft TechNet, modified 2006. Available: <http://www.microsoft.com/technet/archive/security/topics/secaps/authcode.msp>
- McLain, Fred (1997). "The Exploder Frequently Asked Questions (FAQ)". Available: <http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm>
- Seecof, Mark (1997, March). "The real goal of Authenticode" . The Risks Digest v18, Issue 89. Available: <http://catless.ncl.ac.uk/Risks/18.89.html>
- VeriSign (2005). "VeriSign® Code Signing for Microsoft® Authenticode® Technology". Available: <http://www.verisign.com/static/030999.pdf>