Microsoft Authenticode for the

Small Independent Software Vendor

by

Richard Marsden

http://www.winwaed.com

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

MGT.5387-1QA Foundations in Information Assurance, Spring 2006
Graduate School of Management, University of Dallas

Submitted to: Prof. Branden R Williams

20th March 2006

Table of Contents

Table of Charts and Figures

Abstract

Microsoft introduced their Authenticode code signing mechanism in 1996, in answer to an increasing number of malicious web (ActiveX) controls and executable programs on the Internet. Code signing attempts to authenticate authorship by applying a digital certificate to the control or program.

Internet downloads have become the preferred delivery mechanism for small Independent Software Vendors (Micro-ISVs). Authenticode should help to verify that these products are genuine and have not been tampered with, but some Micro-ISVs are reluctant to purchase or use Authenticode certificates.

This paper analyzes Authenticode from the point of view of the Micro-ISV, including both the positive aspects and the perceived flaws. Micro-ISV attitudes and experiences with Authenticode are surveyed.

Overview of Code-signing and Microsoft Authenticode™

Shortly after Microsoft introduced downloadable executable ActiveX™ components, proof-of-concept controls such as Internet Exploder[1] quickly demonstrated that malicious ActiveX controls represented a significant security risk. In response, Microsoft developed its Authenticode code-signing technology as a means of demonstrating the authenticity of specific ActiveX components delivered over the Internet. Authenticode identifies the publisher of the software and verifies that it has not been tampered with[2]. It can also be used to sign executable (.exe) files and other executable components recognized by Windows platforms. Authenticode was first released in 1996 and works with all Windows platforms since Windows 95. However,

[1] McLain, Fred (1996) "ActiveX or how to put nuclear bombs in web pages"
http://www.halcyon.com/mclain/ActiveX/ http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm
[2] Grimes, Roger (1996-2006) "TechNet Archive: Authenticode"
http://www.microsoft.com/technet/archive/security/topics/secaps/authcode.mspx

Authenticode is only switched on as default with Windows XP Service Pack 2[3]. If an end user downloads an unsigned executable, they will now see a warning dialog box similar to that in Figure 1. This dialog box has been described as "scary" by many legitimate software vendors who see it for the first time. It was also the reason that the author quickly implemented code signing for his products.

To sign an executable, a publisher must obtain a digital certificate demonstrating who they are. The digital certificate and matching public and private keys are obtained from a Certification Authority (CA). All of these digital certificates contain the publisher's public key and name, the certificate's expiration date and serial number, the name of the issuing CA, and the digital signature of the issuing CA[4]. Digital certificates may also include the publisher's contact and registration information.

The signing process is outlined in Figure 2. 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.

All certificates have an expiry date. This allows Microsoft or the CA to refuse to renew a certificate if the publisher has proved to be un-trustworthy. Signed executables can also be time-stamped using the CA's online time stamping server, allowing the end user to determine the date

[3] Andersen, Starr and Abella, Vincent (2004). Changes to Functionality in Microsoft Windows XP Service Pack 2; Part 5: Enhanced Browsing Security
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2brows.mspx
[4] Grimes, Roger (1996-2006) "TechNet Archive: Authenticode"
http://www.microsoft.com/technet/archive/security/topics/secaps/authcode.mspx

that the code was signed. In the event of an expired certificate, the date of the timestamp can demonstrate that the code was signed when the certificate was still valid.

The CAs are certified by Microsoft in a hierarchy. Modern versions of Windows are distributed with a number of top-level certificates, although Authenticode also supports the ability to include all certificates from the root to the publisher. This allows a publisher to use a certificate issued by a new second-tier CA whose CA certificates have limited distribution on end-user machines.

Potential Weaknesses

Authenticode has been the subject of quite a bit of criticism. Some of this is due to a misunderstanding of what it aims to achieve, e.g. Authenticode does not and cannot verify that a signed piece of code is 'safe'[5]. However, other criticisms are founded on legitimate weaknesses:

Weak Verification by CAs. When verifying new certificate applications, CAs must avoid issuing certificates to dubious applicants, but they also have a commercial need to make it easy for legitimate publishers to apply for certificates. Requirements vary widely, and typically require a business certificate of some form. Comodo[6] have been known to accept a cancelled check with a DBA ("Doing Business As") certificate issued by a County Clerk. County Clerks do not check DBA applications for trademark infringements, and most banks will create a DBA checking account with only the County DBA certificate. Therefore it would be extremely easy to create the required documentation to apply for a false certificate for all but the most well known organizations.

VeriSign, Inc has stricter controls than Comodo, but they were subject to a much-publicized social engineering attack in January 2001. VeriSign issued two Authenticode certificates with the name "Microsoft Corporation" to a person, who fraudulently claimed to be a Microsoft

[5] Atkinson, Bob (1997). "Comments and corrections regarding Authenticode" *Risks Digest* Volume 18, Issue 85, http://catless.ncl.ac.uk/Risks/18.85.html#subj6

[6] Comodo, Inc http://www.instantssl.com/code-signing/index.html

employee[7,8]. Although the fraudulent certificates could be identified by their date, their existence was embarrassing for VeriSign. Charles Sinclair also reported a bogus Authenticode certificate that was issued by VeriSign to a company called "CLICK YES TO CONTINUE" [9]. This certificate appeared when Sinclair was investigating a pirate software ('warez') website that was pirating his software. Despite being one of the higher-priced CAs, it is clear that VeriSign did not check this certificate's application very thoroughly. Sinclair is not aware of any action performed by VeriSign after he informed them of the certificate[10]. The alternative is that the Authenticode certificate was hacked – something that is reputed to be virtually impossible.

Faulty Implementation. All code is subject to implementation errors. Authenticode has been relatively safe, but vulnerabilities have been found. For example, a patch issued in 2003 corrects an issue in Authenticode that allowed remote code to execute without a warning dialog box under certain conditions[11].

Limiting Microsoft Liability. Mark Seecof argued that Authenticode was intended as a means of limiting Microsoft's product liability[12]. Seecof's argument is that an end user calling Microsoft's help line with a non-functioning computer will be asked if he installed any non-Microsoft software (as signed by Microsoft). If they installed software installed by other vendors, then they must approach other vendors. If they installed unsigned code, then they themselves are responsible. In the nine years since this argument was made, it does not appear to have occurred. It does, however, highlight the need for end user education.

---

[7] Microsoft Security Bulletin MS01-017, http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx
[8] CERT Advisory CA-2001-04, http://www.cert.org/advisories/CA-2001-04.html
[9] Charles Sinclair (ResultsWare Limited) personal communication (March 2006)
[10] *ibid*
[11] Microsoft (2003). MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution, http://support.microsoft.com/?kbid=823182
[12] "The Real Goal of Authenticode", Mark Seecof, Risks Digest Volume 18, Issue 89, 1997 http://catless.ncl.ac.uk/Risks/18.89.html#subj12

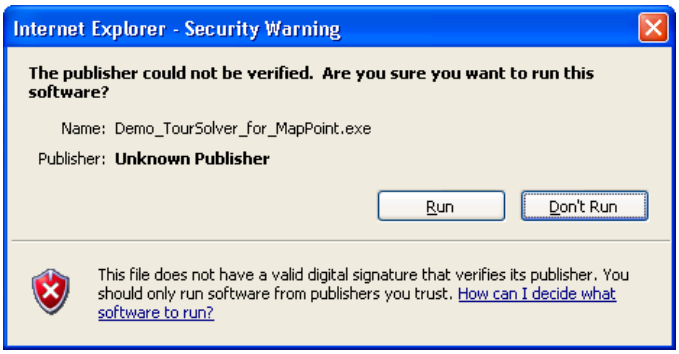


Figure 1, Sample security warning produced by Windows XP SP2 when attempting to run an unsigned executable

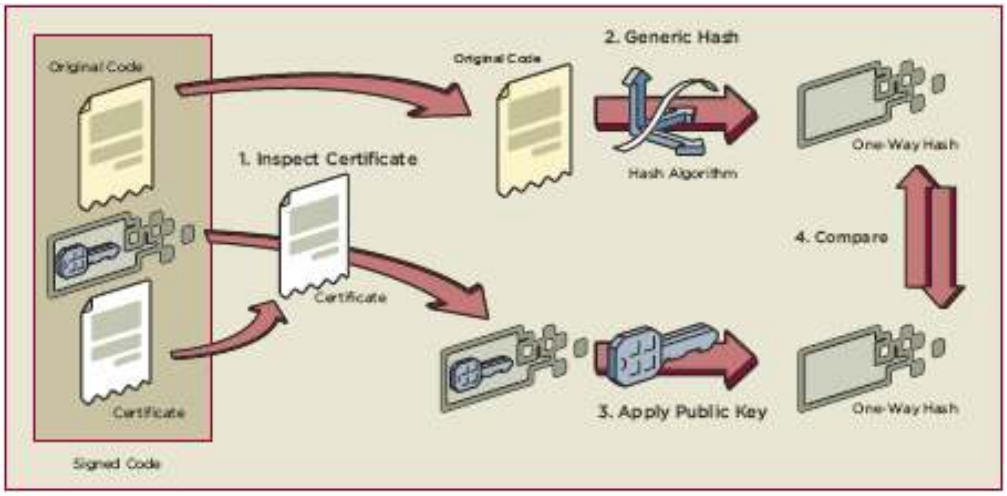


Figure 2,Verifying Signed Code; Source: VeriSign, 2005[13]

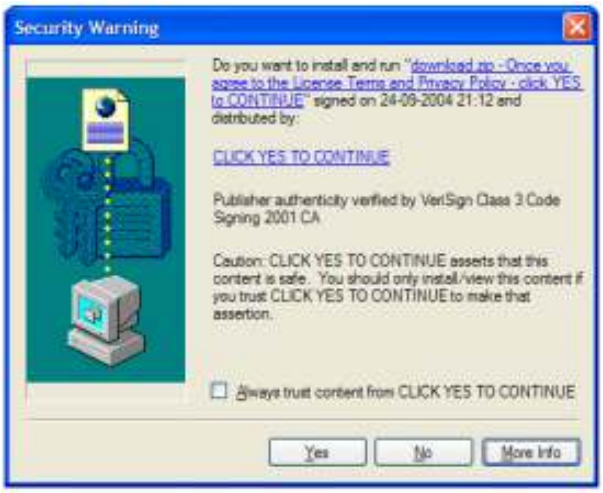


Figure 3, A bogus certificate verified by VeriSign; Source: Sinclair, 2006[14]

[13] VeriSign (2005). "VeriSign Code Signing for Microsoft Authenticode Technology", http://www.verisign.com/static/030999.pdf

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

Micro ISVs Today

The phrase "Micro-ISVs" (Micro Independent Software Vendor) was recently coined by Eric Sink[15] to describe extremely small (typically one person) organizations that write and sell their own software. They have been a notable component of the software industry since the advent of personal computers in the late 1970s, but have risen to prominence with the rise of the Internet and other recent changes in the employment structure of the IT industry.

The shareware industry was born in the 1980s when Micro-ISVs found that traditional distribution channels represented a significant barrier. Micro-ISVs were quick to adapt to the arrival of the commercial Internet in the mid-1990s, and websites became their chief marketing tool. By allowing software to be distributed by downloads, Micro-ISVs immediately had a global and direct marketing channel to potential customers. The Internet distribution model has matured over the past ten years, and the word "trialware" has started to replace "shareware". Larger vendors are also distributing trial versions of their software over the Internet.

With an increasing amount of viruses, worms, spyware, and other malicious downloads, it is extremely important that a Micro-ISV can demonstrate the authenticity of their downloadable software. A potential customer's doubt regarding the bona fide nature of a software download directly translates into lost sales. Although industrial organizations such as the ASP[16] have worked with the Federal Trade Commission in recent workshops[17], individual Micro-ISVs find that they must demonstrate their trustworthiness on their own. Micro-ISVs can rarely afford to build significant brand awareness amongst their target market. A number of independent testing services have been started, but these are virtually unknown to most users and could be easily forged.

---

[15] Sink, Eric (2005) "Exploring Micro-ISVs" http://www.ericsink.com/bos/Micro_ISV.html
[16] Association of Software Professionals http://www.asp-shareware.org
[17] http://www.ftc.gov/opa/2005/03/spywarerpt.htm

Microsoft's Authenticode program should help with some of these problems, especially as it is now switched on as default in the latest Windows XP Service Pack. Although Authenticode does not claim to directly protect from malware written by the certified publisher, it should help to prove that the downloaded software has not been tampered with by a third party. It also gives a form of certified 'real world' identification of the publisher, because the publisher had to present various documents (e.g. certificates of incorporation) to receive the security certificate.

Survey

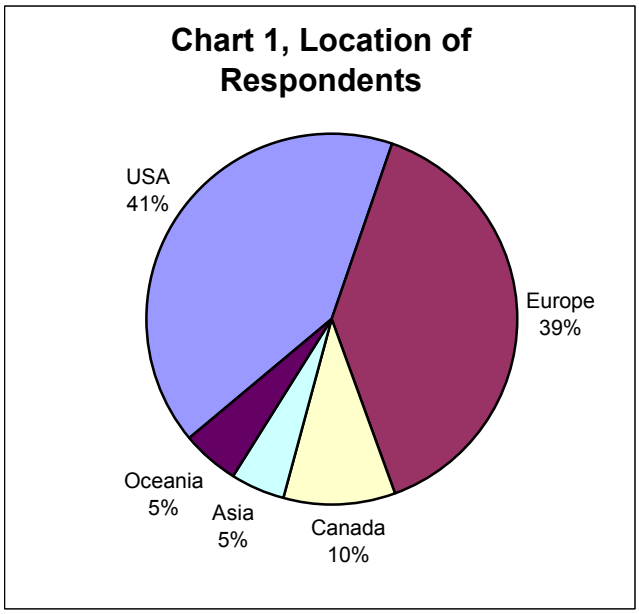
Despite the problems facing the Micro-ISV community today, Authenticode has a mixed reputation amongst Micro-ISVs, resulting in varied acceptance. The author has seen a wide range of views expressed from "I have nothing to lose" through to "it is a protection racket forced on to me by the evil Microsoft". These are only anecdotal comments read on newsgroups and Micro-ISV forums. A survey was designed in order to produce a quantitative sampling of Micro-ISV viewpoints. Is the Micro-ISV community well informed about what Authenticode aims to do, and what its weaknesses are? The survey was also designed to identify any common failings with Authenticode, whether they were perceived or otherwise.

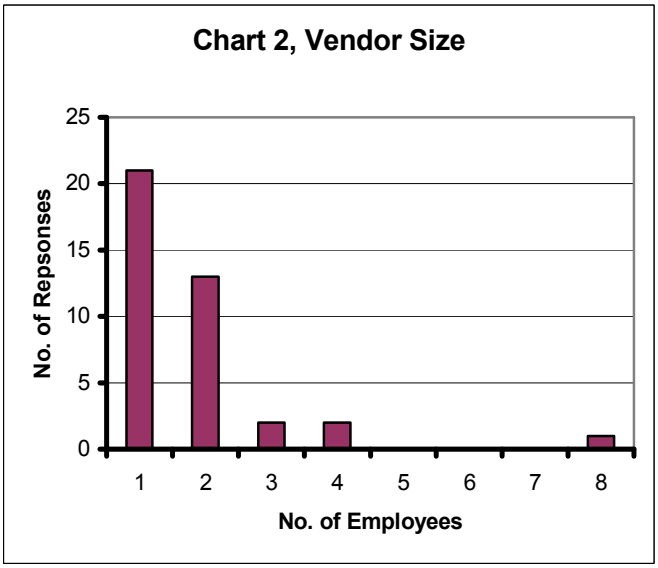
The survey is included in Appendix 1, and ran from 9th February to 9th March 2006. Micro-ISVs were invited from a variety of online forums including those hosted by the ASP, AISIP[18], and newsgroups targeted at shareware authors.

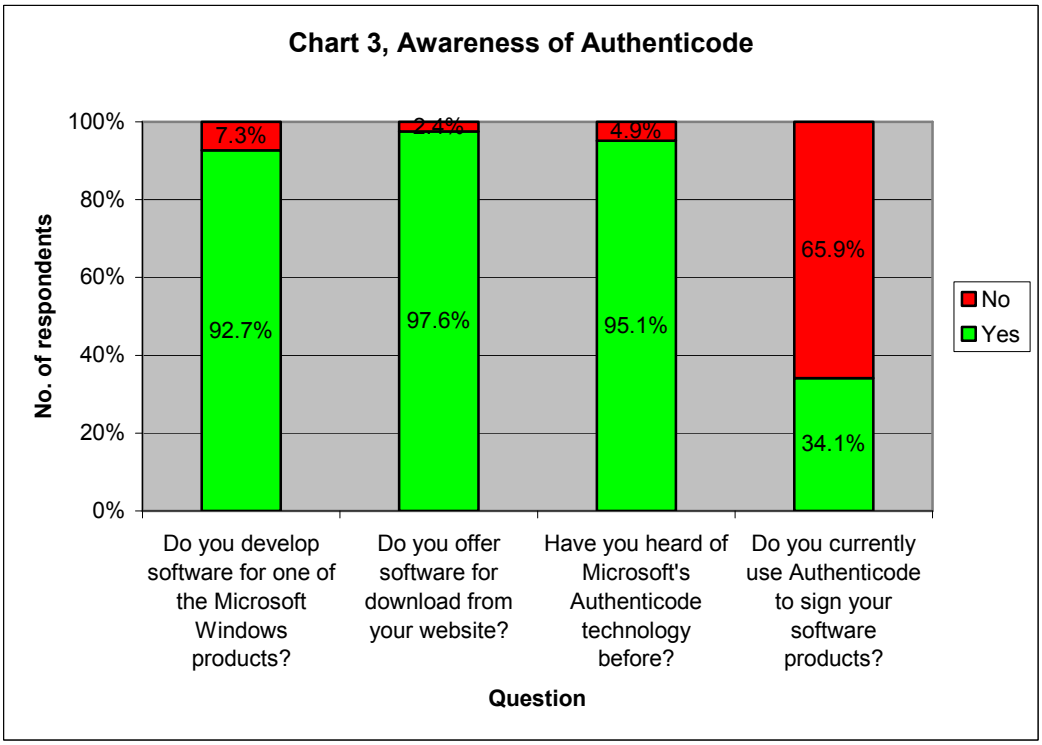
[18] Association of Independent Software Industry Professionals, http://www.aisip.com/

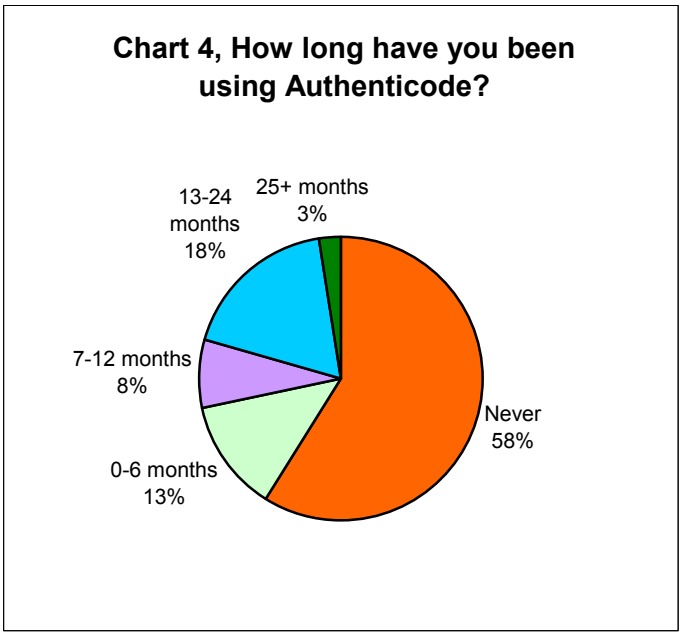
Survey Results

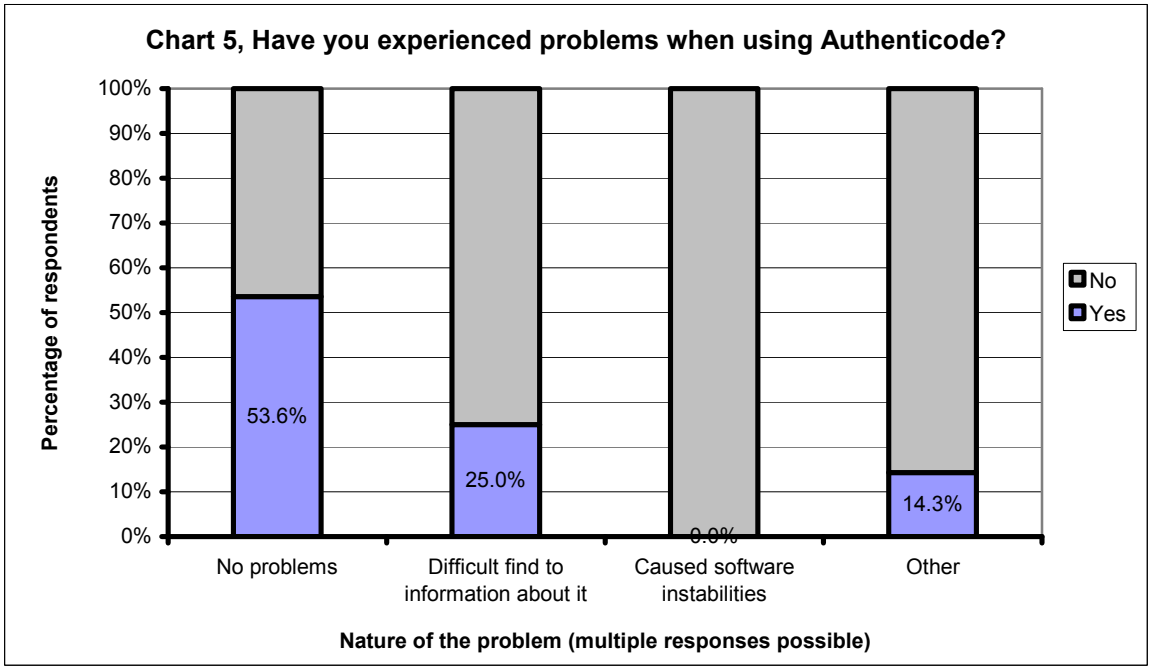
A total of 41 responses were received, and these are plotted in the following charts. General comments were invited, and these are listed in Appendix 2.









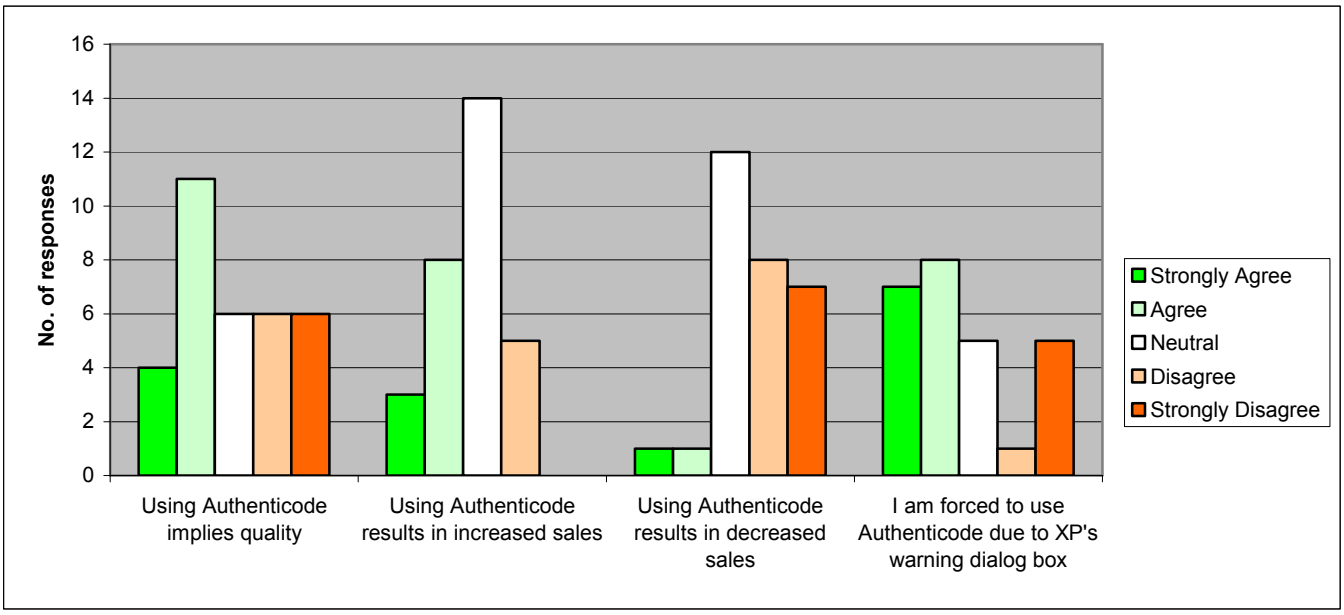


Write-in responses for the 'Other' category were:

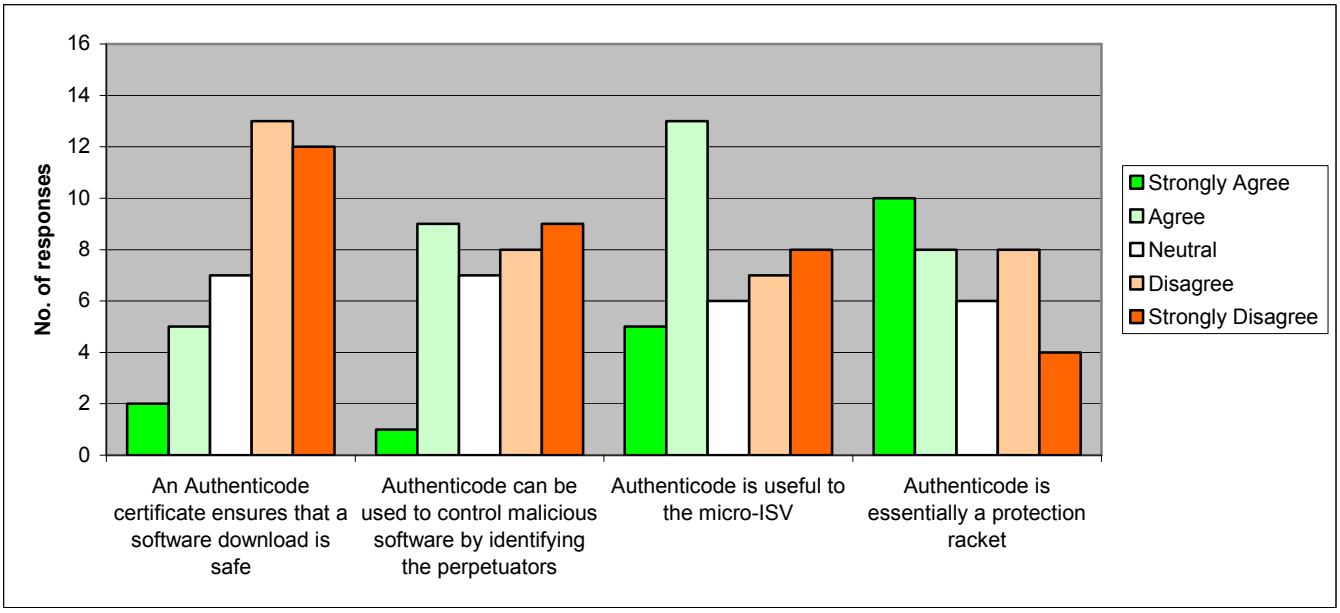
- *Too much effort, costly, and not allowed*
- *Tools are rudimentary*
- *Can trigger ZoneAlarm warnings when signed*
- *Haven't found a way to integrate it*

Chart 6, Statement Responses

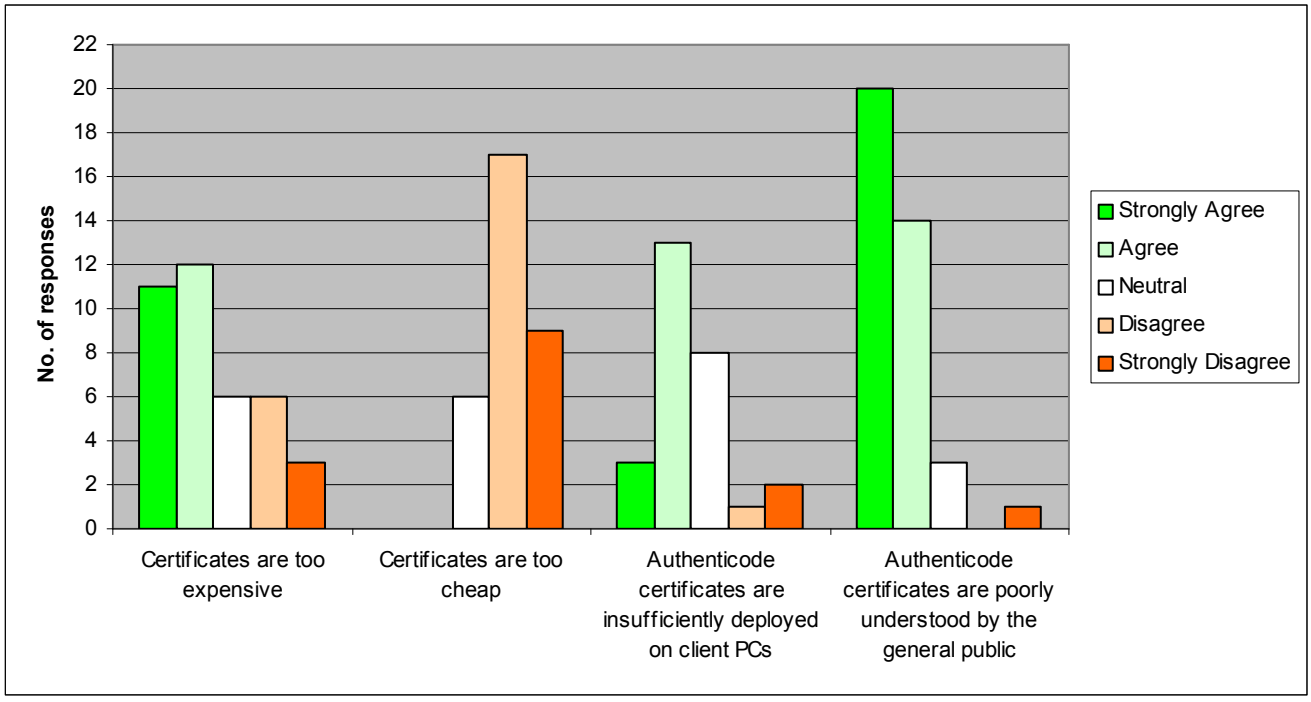
a.)



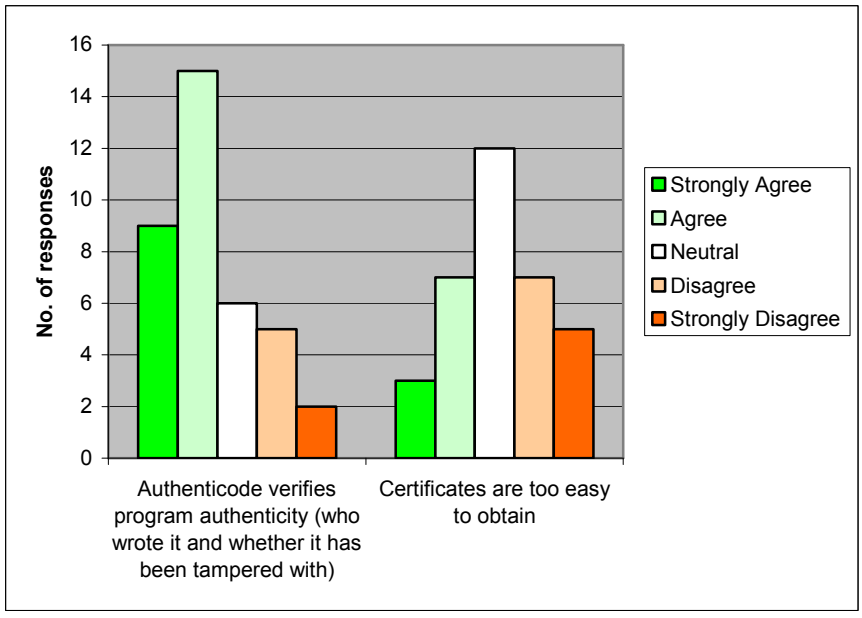
b.)



c.)


No. of responses
22
20
18
16
14
12
10
8
6
4
2
0
Certificates are too expensive
Certificates are too cheap
Authenticode certificates are insufficiently deployed on client PCs
Authenticode certificates are poorly understood by the general public
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

d.)


No. of responses
16
14
12
10
8
6
4
2
0
Authenticode verifies program authenticity (who wrote it and whether it has been tampered with)
Certificates are too easy to obtain
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Survey Discussion

Chart 1 identifies the locations of the respondents. The dominance of the US, Europe, and Canada matches the author's personal observations of the (English speaking) target forums.

Charts 2 and 3 confirm that the survey reached the intended audience of very small organizations who develop software for Windows that is distributed by website downloads. Only five of the respondents were from organizations with more than two employees. Chart 3 shows that 95.1% of respondents had heard of Microsoft Authenticode but only 34.1% actually use it. This confirms and quantifies the reluctance already described.

Chart 4 identifies how long Authenticode had been in use. Note that the discrepancy between those who have never used Authenticode with those who do not currently use it. This is because a small number of respondents have used Authenticode in the past but no longer use it.

As all of the respondents came from online discussion forums, it is likely that many of those who do not use Authenticode, have avoided it because they have heard of problems from those who have. Chart 5 plots the problems that were reported. No one reported software instabilities, although one respondent did comment that they found it caused ZoneAlarm warnings. In contrast, a significant number of responses (25%) found it difficult to find information about Authenticode. The remaining write-in responses all involve usability, with effort, rudimentary tools, and difficult integration all being mentioned. From this one question, it would appear that both Microsoft and the CAs should do a much better job in providing information and increasing the usability of Authenticode for software publishers.

Chart 6 measures the opinion of Micro-ISVs in the form of agree/disagree responses to various statements. Two significant results are on 6b and 6d. Most Micro-ISVs correctly disagreed with the statement that "An Authenticode certificate ensures that a software download is safe" but

agree that “Authenticode verifies program authenticity”. In contrast, only one person strongly agreed with Microsoft’s claim that “Authenticode can be used to control malicious software by identifying the perpetuators”. The remaining responses were divided between ‘Agree’, ‘Neutral’, ‘Disagree’, and ‘Strongly Disagree’.

On average there was weak agreement that “Authenticode is useful to the Micro-ISV” although this was due to a large number of responses for ‘Agree’ that counter-acted a significant number of ‘Strong Disagree’ responses. Twenty-one people disagreed or were neutral on this statement – less than the number of people who did not use Authenticode. I.e. There are people who think Authenticode is a good idea but are not using it yet.

Two statements also examined whether Authenticode directly influenced sales (Chart 6a). Using Authenticode should increase sales due to greater trust on the part of the potential customer. Most respondents were neutral or disagreed with the statement that “Using Authenticode results in decreased sales”, with only two agreeing or strongly agreeing. Less people thought that Authenticode increased sales, although no one strongly disagreed with this statement.

The author occasionally sees comments to the effect that Authenticode is a protection racket. The protection racket label comes from the fact that if you do not pay a CA an annual fee, then your customers will see a warning message. This warranted further investigation. Although fairly even, there was a notable bias towards ‘Agree’ for the statement “Authenticode is essentially a protection racket”. A similar response to the statement “I am forced to use Authenticode due to XP’s warning dialog box”, supported this result. Both statements were supported by further comments in the Comments question (see Appendix 2). Those who think that Authenticode is a protection racket appear to be particularly vocal.

In contrast, there was also a slight bias in agreement to the statement "Using Authenticode implies quality". This is a little contradictory, but all three results are close to even. Also, it is possible for something to imply quality as well as be a part of a protection racket, as outlined in Comment No. 6 (Appendix 2).

There was a very strong agreement with the statement that "Authenticode certificates are poorly understood by the general public". Clearly Microsoft has to further educate the general public (i.e. their end users) about the warning dialog boxes, and their meaning.

Cost could be seen as a barrier and three statements were added to test this. A high cost could be a useful barrier that would discourage many dubious applications, but it could also discourage the small, but legitimate Micro-ISV (e.g. the part time programmer). Three statements were added to test this. None of the Micro-ISVs saw it like this though. The respondents were very neutral regarding the statement "Certificates are too easy to obtain". No one agreed that certificates were too cheap, and most disagreed with this assertion. As expected, this also translated into most agreeing that certificates are too expensive, although some respondents also strong disagreed with this statement. A note-worthy comment was made in Comment No. 9 (Appendix 2). Namely, the cost of an Authenticode certificate is high for a free product. The same applies for bona fide 'hobby' software.

No one likes to say that that they should pay more for something, and it would appear that this feeling was stronger than any thoughts that cost could be a useful barrier to obtaining a certificate.

Conclusions

In order to generate downloads and purchases, Micro-ISVs must demonstrate the bona fide nature of their software. Microsoft Authenticode currently provides the best way of demonstrating authenticity, but it has seen limited acceptance amongst Micro-ISVs. A survey was conducted to determine Micro-ISV knowledge of Authenticode, and reasons for the low acceptance. The survey results confirmed Authenticode's relatively low acceptance by the Micro-ISV community, despite a good awareness of its theoretical strengths and weaknesses.

A significant problem that has been identified is that of communication by both Microsoft and the CAs. Many Micro-ISVs have problems finding information about using Authenticode, and there is a general feeling that the general public is poorly educated about the certificates and related warning dialog boxes.

There was a mixture of opinion concerning the ease of obtaining a certificate. Some found it too difficult or too expensive, whilst others found it too easy. Two examples of fraudulent certificates were identified. This is potentially a very serious problem. Fraud will happen, but Microsoft and the CAs must be very active in identifying fraud cases, revoking fraudulent certificates, and pushing for arrests. For Authenticode to be seen to work, this must be seen to happen. Microsoft and the CAs must be more active in following up reports of fraud and publicizing their activities in this area.

The remaining major problem is that of Microsoft's public image. Although Microsoft's intentions appear to be positive, many people view Authenticode as being a protection racket. These people are particularly vocal in their opinion. It is difficult to counteract this with good public relations, but it could be helped by a high publicity and pro-active approach to verifying CAs, revoking certificates, and even arrests. This would demonstrate that Authenticode works.

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.mspx

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

Appendix 1, The Survey

Authenticode and the Micro-ISV

This survey is about Micro-ISV (small independent software vendor) attitudes to Microsoft's Authenticode code signing technology.

Microsoft introduced their Authenticode code signing mechanism in 1996, in answer to an increasing number of malicious web (ActiveX) controls and executable programs on the Internet. Internet downloads have become the preferred delivery mechanism for Micro-ISVs. By adding a variety of warning messages in operating systems such as Windows XP, Microsoft are actively encouraging the use of Authenticode to sign executable programs. However, many Micro-ISVs remain reluctant to use it to sign their products.

The survey should be completed by only one person from each vendor. The survey reports are to be included in a report for an MBA-level information security course, and will be made available to the public. Individual respondents and companies will not be revealed in the final report.

1. What is the name of your organization? (internal statistical use only, and will not be used in the final report)

2. Where is your business located?

USA	Europe	Oceania
Canada	Africa	
Latin America	Asia	
No Response		

3. How many employees are there in your organization?

4. Do you develop software for one of the Microsoft Windows products?

Yes
No
No Response

5. Do you offer software (ie. trial or full versions) for download from your website?

Yes
No
No Response

6. Have you heard of Microsoft's Authenticode technology before?

Yes
No
No Response

7. Do you currently use Authenticode to sign your software products?

Yes
No
Not relevant for my current platform
No Response

8. How long have you been using Authenticode?

Never
0-6 months
7-12 months
13-24 months
25+ months
No Response

9. Have you experienced problems when using Authenticode? If so, what was the nature of these problems?

No problems
Difficult to find information about it
Caused software instabilities when used with my product
Other (please explain)

Other

10. Please rank the following statements about Authenticode according to whether you agree with them or not.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	No Response
Using Authenticode implies quality	1	2	3	4	5	
Using Authenticode results in increased sales	1	2	3	4	5	
Using Authenticode results in decreased sales	1	2	3	4	5	
Certificates are too expensive	1	2	3	4	5	
Certificates are too cheap	1	2	3	4	5	
The default red warning dialog box in recent versions of Windows XP forces me to use Authenticode	1	2	3	4	5	
Authenticode root certificates are insufficiently deployed on client PCs	1	2	3	4	5	
Authenticode certificates are poorly understood by the general public	1	2	3	4	5	
An Authenticode certificate ensures that a software download is safe	1	2	3	4	5	
Authenticode can be used to control malicious software by identifying the perpetuators	1	2	3	4	5	
Authenticode is useful to the micro-ISV	1	2	3	4	5	
Authenticode is essentially a protection racket	1	2	3	4	5	
Authenticode verifies program authenticity (ie. who wrote it and whether it has been tampered with)	1	2	3	4	5	
Certificates are too easy to obtain	1	2	3	4	5	

11. Do you have any further comments about Authenticode?

12. The final report "Authenticode and the Micro-ISV" will be published online. Please supply your email address if you would like to receive an email when the report is available. Email addresses will only be used for the final report notification, and will be deleted immediately afterwards.

Survey Software Created by WISCO Survey Power.

Appendix 2, Respondent Comments

Question 11 on the questionnaire asked for further comments. The following were received:

1.	Since it's optional, I choose to not use it, or pay Microsoft even more money. I prefer to provide substantial information on my products and services on my Website to give the client a sense of security and reliability.
2.	My responses to 'do you use it' and 'how long' may seem contradictory. I am starting to use it, but it is not on most products so far.
3.	It is a disgusting, criminal racket - they should be free!
4.	Authenticode prevents me from modifying my EXE files on the fly from a Unix website. I would like to track usages, invalidate cracked versions, etc. There are a lot of malicious users out there and Authenticode hamstrings the author from being protected against these users. No thanks.
5.	We don't use authenticode because we see it as a way for Microsoft to extract ca$h from ISVs for almost nothing. We see it as extortion.
6.	It IS a protection racket, and it's too expensive for what it gives you. However, it also is a mark of quality. When I see a signed file, I see that I'm dealing with someone who is serious enough about their business that they spent the $200-$400 to buy the cert. Conversely, if I see an app that DOESN'T have a signature, I am suspicious. Why not? Don't they care what I think? Don't they have $200? Does anyone ever get "busted" for distributing malware that's signed? I would feel better about spending my $200 if I ever heard of somebody's cert being revoked due to bad behavior. Thanks for reading my random thoughts.
7.	Unfortunately, having a stolen signed copy of your code guarantees that it doesn't have something wrong with it added by a hacker. A bit of a double edged sword, because theives can now say "See it's genuine".
8.	Seems like yet another wonderful attempt at getting the world to become a branch of Microsoft Inc. By incorporating a Microsoft technology in to the operating system effectively grants MS an unrestrained monopoly by making it too expensive and too difficult for anyone else to offer a similar signing technology. We need to have some lines drawn as to where the OS ends and the utilities begin. We already have far too much of a co-ercvive monopoly in the basic software industry.
9.	Very difficult to locate signing authority as I'm a sole proprietorship and not a limited company. Also relatively very expensive for my free product.
10.	Most user don't know or care about it. Most don't read the little box that shows up whether it displays a warning or certificate info. If the program is going to be worth something, the process of obtaining the certificate needs to improve, but the cost should be nearly nothing. The certificate fee is essentially covering the cost to verify - in reality they are just collecting money.
11.	For my products, this has been a matter of convenience - the tradeoff between the minor irritation and expense of implementing Authenticode vs. potential questions (w/ associated documentation & tech support) from customers.
12.	Authenticode is a useful tool to provide users with a means to ensure that the piece of software they are using is the same as the one the vendor shipped. In general, software security is built with many layers of which code signing is one of them. In principle, there is nothing to certify that a

	criminal has not obtained the private signing key or obtained a new key through some form of identity theft. There are some interesting issues around trust-based security systems; but I do not currently have time to write here. If you wish to contact me, I may be able to find the name of a man from RSA who has thought about these issues a lot.
13.	When an established vendor/client relationship exists, authentication is of little significance. Where circumstances warrant it, it would be better if supplied by a third party whose success depended upon the reliability and reputation of authentication alone.
14.	I hope by "authenticode" you don't jsut mean the Verisign certificate. If so, then I'd change my "too expensive" answer to "Strongly Agree". The Comodo certificates at $75 (ASP member discount) is low enough to be a no-brainer for me. The only reason I started using code signing was XP Service Pack 2 and that lovely warning. I'm sure it does give the occasional user some sense of security - even if that is a false sense :-)
15.	If you hadn't posted a note saying that Authenicode == Code Signing I would have no idea what this survey is about.