

Can you trust a website?



Graham is a principal analyst specialising in IT security and business continuity

Graham Titterington
London

A lot of attention has been given to identifying and authenticating users of online services, and particularly when large sums of money are at risk. But now there is a need for two-way authentication, as malicious websites have become the main conduit for both information theft and the distribution of malware. Much less effort has been devoted to protecting users from these sites than to authenticating users to sites. A UK start-up company has developed a simple and rugged approach to countering spoof sites, that is under the control of the legitimate site operator and can significantly improve the security of Internet users.

Malicious websites are big business

Cyber crime is about fraud and theft. Hackers seek to steal users' credentials for accessing online banking, government gateways, retail and other critical sites where they might have the opportunity to steal from the victim. Most hacking attacks now involve malicious websites, either as a vehicle for downloading malware onto the victim's computer when they visit the site, or by posing as a legitimate site. Hackers entice users to go to these sites by sending links in email messages, by router poisoning or by corrupting a link in a page of a legitimate site.

The problem of malicious web pages has grown as hackers have turned to corrupting websites of legitimate

organisations. Users used to be safe if they took care about which sites they visited. This is no longer the case. The problem is exacerbated by the slowness of some organisations in rectifying pages that have been hacked, even after security companies have informed them of the problem.

The URL displayed in the browser is the main check that the user is at the correct website. However, experience shows that most users do not check this, and indeed most would not understand if they were in the wrong place. This perception has been confirmed by research carried out by MIT and Carnegie Mellon University in the US, which showed that even highly educated users do not check or understand the information in the periphery of the browser screen. Hackers often add to this confusion by choosing a URL that has something in common with the legitimate address. A more proactive form of protection is needed.

The industry's response

The industry has produced a relatively small range of responses to this need, probably because the number of vendors in the browsing arena is small. Although there have been advances in the last two years, the onus of checking has remained on the user. In many cases the protection does not kick in until after the user has downloaded the malicious page, by which time the damage may have been done.

There have been three broad categories of approach to protection:

- website certificates
- in-browser protection
- website reputation filters.

Website certificates have been around for many years and are characterised by the padlock icon on the browser screen. The industry has lacked a

clear focus on assurance levels. Each certificate issuer has its own procedure for authenticating an organisation before it issues the certificate, and this may amount to no more than matching the site to an email address. Users do not understand what they mean, or how to detect a fake certificate.

In early 2007 VeriSign, the market leader, attempted to raise the bar by introducing Extended Validation (EV) certificates that are only issued to companies that VeriSign has rigorously validated. Recent browsers, such as Internet Explorer 7, display the URL of a page with an EV certificate against a green background to reassure users. However, EV certificates are still not widely used and even the major banks only use them on a handful of particularly sensitive pages; the main body of their website is not protected by EV certificates.

Furthermore, users can be confused when a company's trading name differs from its legal registration name. For example, the Get Safe Online site that offers advice on safe Internet use is not, as popularly believed, operated by the UK government. The site certificate says it belongs to Endurance Ltd, the little known operator of the site. This is meaningless to users who do not know the contractual arrangements covering the provision of this service.

Browser vendors are becoming increasingly involved in protecting users from visiting malicious websites. For example, Internet Explorer 8 contains many security enhancements, including click-jacking protection. The existing anti-phishing filters in IE7 will be extended to detect malware on web pages. IE8 will highlight parts of a URL where it suspects the user has been diverted to a different site from the one they thought they were accessing. There will also be features to protect against the non-persistent Type 1 cross-site scripting attacks.

The Mitre Corporation, a not-for-profit organisation sponsored by several US government agencies, has reported that Type 1 XSS vulnerabilities are now the most common class of vulnerability and are found in many popular websites. In many respects Microsoft is catching up with other browsers. The feature that is supposed to recognise malicious

websites should block about 80% of them, but there will be problems keeping the list up to date and about 20% will get through.

All the leading anti-malware vendors now provide products and services that monitor the Internet and check for malicious content (website reputation

filters). The problem is that they only protect users who have bought the relatively expensive products and kept their subscription up to date. Website operators cannot assume that all their customers will have this protection and, in many cases, the cost of a breach falls as heavily on the website operator as it does on the end user.

First Cyber Security

First Cyber Security (FCS) was set up in 2004 to provide a simple-to-use way of authenticating websites and enhance user confidence in online transactions. Its approach offers several advantages:

- Simplicity for the end user, coupled with reliability, is the overriding design objective.
- The service does not depend on end users having any other security products or services on their PC.
- The website status is delivered outside the browser in a way that is visible, clear and unambiguous, based on the red, yellow and green traffic-light model.
- The software is sold to website owners as a subscription service, and they distribute the client widget to their customers free of charge.
- Website authentication is very strong. It is based on several attributes of the web domain. This information is encrypted, making it virtually impossible for a spoof site to simulate the attributes.
- Access to a spoof site can be blocked within minutes of it being identified.

Applications and markets

FCS has been selling this service for nearly a year and most of the first tranche of adopters have been in the UK public sector. Financial services and the media are also showing

interest in the technology. These are the sectors where hackers are most likely to target their attacks because they offer opportunities to steal money and personal information that can be used for subsequent frauds. Spoof media sites can be used for campaigns of disinformation, based on the trusted brand of the site. E-commerce sites could also benefit from enhancing the confidence of their customers. FCS plans to expand into a wider geographical market in the later part of 2009.

First Cyber Security's offering

FCS sells a managed service to websites. This includes a widget that they supply to their end-user customers free of charge. A customer's PC user only needs one widget for all the websites that are protected by FCS. The widget creates a tiny window that is always visible over any other windows on the screen, and which appears in the same place until the user moves it. The user knows where to expect to see it. It displays:

- the logo of the organisation that owns the site
- the name of the user
- a green, yellow or red indicator of the website's provenance. Green means the site has been positively authenticated, yellow means that it has not been authenticated (it is not in the FCS database) and red

means that the organisation hosting the legitimate site has notified FCS that the site is a known spoof site. Access to red sites is blocked.

End users are supplied with an encrypted copy of part of the FCS domain database, which is guaranteed to be updated by a polling mechanism within 30 minutes of a website owner changing its master data. This allows organisations to protect their customers much more quickly than is possible without the service – it can take 72 hours to close a phishing site, and then the hackers migrate to a different IP address and start again. Only information about domains used by the end user is downloaded to their PC to minimise the size of their copy of this database. It is automatically extended when they access a new domain within the FCS customer base. Any tampering with the FCS client immediately changes the appearance of the user screen.

