Data is playing a increasingly important part in the global economic landscape. That’s indisputable. With the increase in data comes a new demand on businesses to be able to consistently store more and more information. As companies seek to use this information as a commodity to gain insight into consumer behaviour, the need for more secure internal and external services arises.

Over the last decade, the popularity of e-commerce and the use of websites and web servers as a means to both inform consumers and perform commercial transactions has grown enormously. But back in the early 2000s, there was little in the way of publicised security research on the vulnerabilities of web servers.

Today, there’s no room for a ‘set it and forget it’ mentality when it comes to security. Administrators must track attacks, mitigations, patches and recommended configuration changes if they want secure websites and web servers. As consumers become more wary about giving out their data, having a secure site has become increasingly necessary.

“If you have an e-commerce site and you’re dealing with customers, you’re dealing with end users and you need to take in their information, and you want to take in their information in a secure manner. A poor site can invade their privacy,” said Bruce Morton, director of certificate technology and standards at Entrust Dacard.

Over the past 20 years, cipher (encryption) security has been moved ahead by developing new Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols, migrating from 1024 to 2048-bit RSA keys and from the SHA-1 to the SHA-2 hashing algorithm. Since the mid-1990s, the SSL/TLS industry has developed six versions of the protocol. The SSL protocol was originally developed by Netscape and the protocol development was moved over to the Internet Engineering Task Force (IETF) which created TLS. In 2004, SSL 3.0 and all TLS versions were generally supported. These protocols essentially allow consumers to know whether or not they’re using a valid site.

“To protect the information [on your customers’], you basically create a key pair: a private key and a public key. A private key is what’s going to be used to encrypt information from the server’s point of view. We provide the public key to a certification authority, like Entrust, and we basically tie that public key to the identity of the site and to the domain name that we want to protect. So now when a browser goes to the site, it gets to use that certificate and it allows the browser to authenticate that that’s a valid site,” said Morton.

As the research into and modification of the SSL and TLS protocols has increased, many security exploits have been discovered.

Protection from attacks
In the past few years, there have been multiple attacks on the SSL/TLS mechanism, with a memorable variety of names such as Beast, Crime, Freak, Logjam, Lucky Thirteen and Poodle. These attacks have various effects depending on what kind of attack is performed, but ultimately they will allow unauthorised access to information in one form or other.

“They basically allow someone break the encryption and either view the information or change information. In some cases, they can start creating their own transactions that look like they were created by the server, where the owner of the server then trusts those transactions when it was actually an attacker,” said Morton.

The wide-ranging effects of these attacks, combined with the consistent need for migrations as SSL/TLS has evolved, means that today we are seeing more servers which are not properly set up, have not mitigated known vulnerabilities and do not meet best practices. To assess how well Irish companies are adhering to these best practices, Entrust Dacard surveyed the top 100 indigenous companies headquartered in Ireland from the Irish Times Top 1000. Using the Qualys SSL Labs tool, SSL Server Test, each company was given a grade based on the SSL Server Rating Guide.

Of the 100 companies surveyed, only 57 were protected by SSL/TLS. Of those 57, 81 per cent have not deployed the more secure Hyper Text Transfer Protocol Secure (HTTPS) on their home page.

From this data alone, it was clear the average Irish company does not yet support the ‘Always-On SSL concept inherent to properly configuring and maintaining SSL/TLS.’

Always-on security
Always-On SSL, or HTTPS Everywhere, is a concept where the whole website is protected by HTTPS. Always-On SSL is a fundamental, cost-effective security measure for websites that helps protect users from the beginning to the end of a web-based transaction, making it safer to search.

The survey says...
Entrust’s survey of Irish businesses’ online security showed Ireland is behind on best practices in the area. There’s room for improvement, writes Aoife Valentine.
share, and shop online.

Companies which implement Always-on SSL will use so through SSL certificates purchased from a trusted Certificate Authority. This basic, easy-to-implement authentication measure provides security by explicating the identity of the website and encrypting all information shared between it and the user (including any cookies exchanged), and protecting that data from unauthorised viewing, tampering, or use.

Though many companies can implement SSL/TLS certificates, it’s a matter of whether or not it was done correctly and according to the best practices that determine the grade it gets on the guide.

“We have certain criteria for setting up the server and I think when we look at the analysis, did they put in the right cipher suites to protect the transactions? No they didn’t. Did they put it in the right cipher suites to protect the transactions? No they didn’t. That’s the item that the server owner has control over. What server does he buy? Do they keep it upgraded? Do they con- figure it properly to set these up? It’s completely exclusive from the certificate itself. The certificate will work in basically almost anything they put together, but did they put it together properly and does it have the highest security?” said Morton.

From the survey’s results, 83 per cent of the servers didn’t completely support forward secrecy, which mitigates the pervasive surveillance attack found from the Edward Snowden data. 77 per cent didn’t use or accept the weak RC4 cipher, and 48 per cent didn’t support TLS 1.2, the most current version of the protocol. Together, 25 of the businesses surveyed support SSL 3.0 or SSL 2.0, both of which are obsolete and insecure versions of the SSL protocol.

The SHA-1 signed certificate, a cryptographic hash function used to determine data’s integrity, was used by 38 per cent of businesses, but SHA-2 is the more recent version.

In most cases, Chrome will present an error with SHA-1 certificates. Also, SHA-1 will not be supported by Windows in 2017. TLS fallback was allowed by 37 per cent of businesses, which could allow a server to be deprecated to SSL 3.0 and become subject to a Poodle attack. The study found that 10 per cent of businesses surveyed were vulnerable to Poodle attacks, while Logjam attacks might not be mitigated by the 33 per cent of businesses supporting the weak DH cipher.

Though these statistics suggest that Irish websites are perhaps quite vulnerable to various different attacks, Morton was keen to emphasise that there is a difference between identifying vulnerabilities and attacks.

“Most of these are vulnerabilities and not attacks. Almost every one of these was found by a researcher and not found by an attacker. We exchange the two things together but most of these things, we’re just trying to get them to fix them before they’re used in attacks,” he said.

Bruce Morton, director of certificate technology and standards at Entrust Datacard

Strong verification

Extended Validation Certificates (EV) are public key certificates, which are issued according to a specific set of identity verification criteria, requiring extensive verification of the requesting entity’s identity before a certificate authority (CA) will issue one. Only four of the businesses surveyed had an EV SSL certificate installed, despite the fact these certificates are very valuable in terms of proving a site’s identity and preventing phishing scams.

This type of certificate is very beneficial for sites susceptible to phishing attacks and is typically found on financial and e-commerce driven websites.

EV is also a great certificate for building brand trust. By all indications, EV certificate benefits are not well known to the Irish IT web development and any other communities that are responsible for website and server maintenance.

“If you go to the site, you’ll see a green indicator up in the browser status bar, over the name of the site,” said Morton.

Bruce Morton, director of certificate technology and standards at Entrust Datacard

You have huge phishing targets like PayPal, but an attacker can’t get an EV certificate that lines up with the PayPal web address and the attacker can’t get an EV certificate for your favourite bank’s name and domain name

Strong verification

Extended Validation Certificates (EV) are public key certificates, which are issued according to a specific set of identity verification criteria, requiring extensive verification of the requesting entity’s identity before a certificate authority (CA) will issue one. Only four of the businesses surveyed had an EV SSL certificate installed, despite the fact these certificates are very valuable in terms of proving a site’s identity and preventing phishing scams.

This type of certificate is very beneficial for sites susceptible to phishing attacks and is typically found on financial and e-commerce driven websites.

EV is also a great certificate for building brand trust. By all indications, EV certificate benefits are not well known to the Irish IT web development and any other communities that are responsible for website and server maintenance.

“If you go to the site, you’ll see a green indicator up in the browser status bar, over the name of the site,” said Morton.

Bruce Morton, director of certificate technology and standards at Entrust Datacard

You have huge phishing targets like PayPal, but an attacker can’t get an EV certificate that lines up with the PayPal web address and the attacker can’t get an EV certificate for your favourite bank’s name and domain name

Strong verification

Extended Validation Certificates (EV) are public key certificates, which are issued according to a specific set of identity verification criteria, requiring extensive verification of the requesting entity’s identity before a certificate authority (CA) will issue one. Only four of the businesses surveyed had an EV SSL certificate installed, despite the fact these certificates are very valuable in terms of proving a site’s identity and preventing phishing scams.

This type of certificate is very beneficial for sites susceptible to phishing attacks and is typically found on financial and e-commerce driven websites.

EV is also a great certificate for building brand trust. By all indications, EV certificate benefits are not well known to the Irish IT web development and any other communities that are responsible for website and server maintenance.

“If you go to the site, you’ll see a green indicator up in the browser status bar, over the name of the site,” said Morton.

Bruce Morton, director of certificate technology and standards at Entrust Datacard

There’s more information in the certificate in order to tell you who they are, what jurisdiction they were formed in and they’ve gone through a much higher validation process so that we also really know that the issuance of the certificate was strongly validated,” said Morton.

“But from the user’s point of view, and one of the main reasons we created this was to mitigate against phishing sites.

“You have huge phishing targets like PayPal, but an attacker can’t get an EV certificate that lines up with the PayPal web address and the attacker can’t get an EV certificate for your favourite bank’s name and domain name. We’re been doing this since 2007 and the main aim is to see that green bar over and over again and that’s what consumers get used to seeing. If they go to a site and it’s not there, hopefully they see there’s something wrong and they try again,” he said.

No A+ websites

Though no business was awarded an A+ grade, four scored an A and two scored an A-. To receive an A+, a site must support HTTP Strict Transport Security (HSTS). HSTS is a relatively new technology. Servers using HSTS send a header to the browser stating that the website should only be presented with HTTPS.

The header also provides a time period, the data from which can be stored on the computer accessing the website. In the future, if the user goes back to the site and it is no longer supporting HTTPS, then the browser will present an error. More adaptation of HSTS will occur when administrators become educated and servers support HSTS.

“In the scoring system, some of the sites are ‘pretty good…but’. And when they fail ‘the but’, it brings them from an A or B or C to an F,” said Morton.

Twelve scored a B, 15 scored a C and 19 scored an F. In the B grade, the main issue was weak Diffie-Hellman support. The Diffie-Hellman (DHE) algorithm provides the capability for two communicating parties to agree upon a shared secret between them. It’s an agreement scheme because both parties add material used to derive the key. The shared secret can then be used as the basis for an encryption key to be used for further communication. Also six firms support the weak RC4 cipher.

In the C category, ten of the servers didn’t support TLS 1.2, the strongest version of the SSL/TLS protocol. Four supported the weak RC4 cipher previously mentioned. While in the F category, ten websites supported only SSL 2.0, despite best practices indicating that it’s best not to support SSL 1.0, 2.0 or 3.0, as TLS is the preferred, safer protocol today.

Five of the servers in the F category hadn’t mitigated Freak attacks, four hadn’t mitigated Poodle against TLS and four were vulnerable to man-in-the-middle.
The fact we can access their web pages gives us a snapshot review of how they do things. If this is how they present the front on house, what’s going on behind the front door?

Neil Foxley, Entrust Identity Guard Cloud Services

big difference is the certificate authority has standards and must meet, compliance rules they have to meet, and audits they have to meet. When you do it yourself, you can make up your own rules, hypothetically. You might get the lock, but you don’t get any quality. The cert that is issued from an authority, the quality is forced in. We all have to meet our standards and all get audited on an annual basis. We have to prove that we meet the standard so it really raises the bar for security if it’s issued from a publicly trusted CA,” said Morton.

Neil Foxley, channel manager for Britain, Benelux, and Eastern Europe for Entrust IdentityGuard Cloud Services, said more needs to be done in Ireland to provide privacy, increase SEO, increase benefits across the board to both the business certificates such as EV or multi-domain name.

Finally, the best practices methodology will recommend that the website implement Always-On SSL. Always-On SSL will help mitigate known security vulnerabilities (for example, Firesheep and SSLstrip). MITM and protect user privacy. HTTPS will increase the websites’ Google ranking, which will bring more users to the site. In addition, if you want to increase your website performance with HTTP/2, you will need HTTPS enabled to be able to integrate with almost all modern browsers. Simply put, Always-On SSL will protect your users and will support the increased performance of your website.

Ireland lags behind

While these best practices are the ideal, Ireland hasn’t quite reached this standard yet. We need to stop asking the question, do we need an SSL/TLS certificate? In today’s age there’s few instances in which businesses won’t require this level of security, even where there is no e-commerce functionality on the site.

Neil Foxley, channel manager for Britain, Benelux, and Eastern Europe for Entrust IdentityGuard Cloud Services, said more needs to be done in Ireland to provide privacy, increase SEO, increase the site’s performance, providing benefits across the board to both the business certificates.

But perhaps more tellingly, according to Foxley, the level of security may suggest how seriously the organisation takes its business, which is something to seriously consider.

“There’s room for improvement [in Ireland]. This is no longer just an e-commerce type site problem. You can argue that if they don’t take their website certificate seriously, do they take their internal certificates seriously as well. The fact we can access their web pages gives us a snapshot review of how they do things. If this is how they present the front on house, what’s going on behind the front door?” said Foxley.

MTM attacks. There were also five sites rated M or T, meaning their SSL/TLS certificate either had a mis-matched name, or was not trusted.

A name mis-matched happens when the common name to which an SSL Certificate is issued (for example, www.example.com) doesn’t exactly match the name displayed in the URL. However, the test results from these sites were not included in the analysis.

Though 19 sites scored an F grade, these aren’t sites the public need to avoid or would even necessarily know to avoid, according to Morton.

“The end user doesn’t know what they scored. They would have to do all their own research to figure out the score. In a lot of cases, that site might support SSL 2.0, SSL 3.0, TLS 1.0, 1.1 or 1.2, it might support all of those things and someone comes in with a browser and the browser supports TLS 1.2 and it all works fine, but the problem is there might be a way to degrade it down to SSL 3.0 or SSL 2.0 and that level can be broken,” he said.

“In all cases the user won’t even know and will only have an issue if they’re pulling out their Windows XP computer with Internet Explorer version 6 on it, but if you’re using Windows 7, 8 or whatever and you’ve the latest and greatest browser version, you’ll probably be protected on those F sites. It’s scoring an F really because it can be degradable to someone that’s using bad browser software.”

Room to improve

On the positive side for Irish security, over 50 per cent of the companies were supporting SSL/TLS. In most cases however, they could be upgraded to close known security holes. And in addition, the other 43-48 per cent of websites that were not using SSL/TLS need to look at implementing the protocols to protect their users and increase their search engine optimisation.

The top two major issues noted in the survey is that servers are not configured properly to support the newest versions of the protocols and cipher suites. The survey also showed us that many Irish servers are still supporting the SHA-1 hashing algorithm.

In general, there needs to be a better way to educate web server administrators, for the administrators to know how well their server is functioning, and there also needs to be a process or a methodology to allow administrators to have a model to continually support their servers.

Any administrator’s best bet in this case is a reliable Certificate Authority. The CA will act as a partner to help support the implementation of a secure server. The CA will perform certificate verification, issue certificates, provide renewal notices, renew certificates, revoke compromised certificates and provide certificate status information to all of company users.

The CA will keep track of and meet industry requirements and will prove compliance through annual audits. The CA will also provide educational tools and an SSL/TLS best practices methodology to configure servers and mitigate vulnerabilities.

“If you’re trying to protect user information then you need a certificate. If you’re going to use a certificate, you can create one yourself, it’s possible to create one yourself, or you can get one from a certificate authority. The

when you put information into the status bar, the domain name and everything, but you might be able to add in other characters there that will make the site do some other function. You didn’t know it, you didn’t design it that way, but you’ve left yourself open to a vulnerability,” said Morton.

The best practices method will focus on enhanced server security, and it should discuss domain protection. The methodology should provide information so that the administrator can be coached to use better way to educate web server administrators, for the administrators to know how well their server is functioning, and there also needs to be a process or a methodology to allow administrators to have a model to continually support their servers.

Any administrator’s best bet in this case is a reliable Certificate Authority. The CA will act as a partner to help support the implementation of a secure server. The CA will perform certificate verification, issue certificates, provide renewal notices, renew certificates, revoke compromised certificates and provide certificate status information to all of company users.

The CA will keep track of and meet industry requirements and will prove compliance through annual audits. The CA will also provide educational tools and an SSL/TLS best practices methodology to configure servers and mitigate vulnerabilities.

“If you’re trying to protect user information then you need a certificate. If you’re going to use a certificate, you can create one yourself, it’s possible to create one yourself, or you can get one from a certificate authority. The

when you put information into the status bar, the domain name and everything, but you might be able to add in other characters there that will make the site do some other function. You didn’t know it, you didn’t design it that way, but you’ve left yourself open to a vulnerability,” said Morton.

The best practices method will focus on enhanced server security, and it should discuss domain protection. The methodology should provide information so that the administrator can be coached to use