The Centre for Public Safety

Public Safety Briefing October 2016

Secure Foundations: Assessing the cyber-security of UK policing's online presence

Digital transformation in public services relies upon secure foundations. With huge potential for transformation within policing, The Centre for Public Safety has examined the public-facing digital infrastructure to test these foundations. The results highlight areas for commendation and concern.

Research Overview

- We scanned 71 police and affiliated websites (including our own) and found that just over one-quarter (27%) demonstrated the highest world-class standard of secure connection, the remainder (73%) either lacked a secure connection for visitors or their implementation was deemed deficient or insecure.

- Almost one quarter (24%) of the sites lacked any automatic secure connection, meaning information is communicated in plain unencrypted text across the internet. Of these, more than 70% (12 agencies) invited users to submit personal data - and in some cases information specifically relating to criminal activity - via these unsecured connections. They are exposing the public to unnecessary risk.[1]

- This is despite the fact that the use of secure connections when transmitting personal data is regularly highlighted in crime prevention and online safety advice ("look for the padlock") issued by the police service, Government and industry partners.[2]

- Around 1 in 10 were found to have significant vulnerability in their implementation of a secure connection - including the National Crime Agency's Child Exploitation and Online Protection Centre (CEOP), which has a specific online focus, along with six territorial police forces.

- There appeared little connection between total spend on technology and performance in our assessment. The Metropolitan Police which spent in excess of

[1] See pp.3-4 for examples of the potential risks the public are being exposed to.

[2] Get Safe Online - https://www.getsafeonline.org (Accessed 7 July 2016)

£110 million on just one IT supplier in 2014/15 only obtained a grade C.[3] At the other extreme, smaller forces, such as Dorset, Durham and Warwickshire, with much more limited IT budgets achieved commendable A grades, suggesting that big doesn't mean beautiful when it comes to policing and IT.[4]

- Some of the newest implementations fell short of the highest world-class standards. Cheshire Constabulary's new "upgraded" website saw it drop from a C grade to an F grade. Meanwhile the Home Office's online crime reporting and terrorism/extremism reporting tools only achieved a B grade.
- The latest iteration of ActionFraud - for the reporting of phishing and malware - and the College of Policing's NCALT e-learning service (used to train new and existing police officers and staff) both fared worse, attaining C grades.
- While some may suggest that the likelihood of a malicious actor seeking to intercept communications between the public and bodies charged with their safety is very small, the risk itself is unknown. Individual communications in isolation may be of little value, but if a malicious actor was able to intercept communications on-demand and/or at scale then the potential public harm is significant.
- This relatively simple scan of public-facing UK digital policing security is necessarily simplistic. As we outline in our methodology, the security of a service consists of far more than the implementation of a secure implementation of the technology that encrypts online communications (SSL/TLS).
- Our scan highlights what might be considered a proxy for the general security of the police's public-facing digital infrastructure. If SSL/TLS implementations are deficient, what other – less visible – areas may be deficient or insecure?
- This work provides an insight to how seriously UK policing is taking the growing threat and provides a benchmark for future comparison - and for leaders within policing to assess their agency's performance.
- It is right to commend the 27% of forces and agencies that have achieved the best gradings - especially those that have also commenced the delivery of online pathways for the public to interact with them.
- With cybercrime both under-reported and a growing threat, the state of much of the infrastructure suggests both significant room for improvement and a failure on the part of some leaders to grip and/or successfully devolve the delivery of their technology and cybersecurity.

[3] FOI Request, Metropolitan Police Service (March 2016)

[4] The Centre for Public Safety will be publishing further work on police IT successes and failures.

- Whether in-house or outsourced, it appears that some continue to fail to provide the foundations for the digital transformation that our police forces are both seeking to achieve and expected to deliver.

The public expect communications with the police to be conducted securely and with a right to privacy. Secure-by-default signals a commitment to that expectation.

- The public expect communications with the police to be conducted securely. When calling 101 or 999 (or 911), the public do not expect individuals to be able to eavesdrop on the telephone call. The public, quite rightly, have the same expectation with regards online communications with the police.

- The A-graded delivery of 'secure-by-default' by 17 police forces demonstrates that some forces and their IT partners recognise the need to both signal and deliver a secure communications channel. Those sites with room for improvement can and should aspire to reach the same standard.

- Consider the following examples in which a failure to implement securely encrypted connections could undermine public trust and public safety:

Example: Young man provides information on a stabbing and drug dealing

Connor has information relating to local drug dealing and associated violence. After the recent stabbing of a close friend in a case of mistaken identity, he wants to help police by providing some information.

Connor wants to avoid any retaliation for "informing" and decides to use an internet connection at a nearby coffee shop. He connects to the public Wi-Fi and visits the local police force website. He finds a form appealing for information about crime in the area. Believing he is secure, Connor fills in the form and provides information of significant value to the investigation into both the stabbing and local drug dealing.

The police website does not make use of a secure-by-default connection and the information was transmitted in plain text. Jason is also in the coffee shop that day, he uses the busy venue to "sniff" credit card numbers which he then uses to furnish local gang members with luxury hire cars and other resources.

Recognising the value of the data he has intercepted, Jason sells it to the local gang. The gang identify Connor and that night they ambush him on the estate and stab him repeatedly in the buttocks and slash his face. They finish by scrawling the words "snitches get stitches" across Connor's front door.

Example: Young woman in a coercive and controlling relationship seeks help

Debbie has been subjected to coercive and controlling behaviour over a number of years by her long-term partner, Steve. Debbie has never called police but one day reaches breaking point and decides to find out what help might be available. Debbie knows Steve has some sort of spy software installed on the home tablet and desktop computers, so secretly buys a small smartphone from the local market to help build an escape plan.

Debbie gets home, and while Steve is out, she connect the phone to the home Wi-Fi and visits the local police website in the hope of finding out what help may be available. Debbie reads about new legislation that makes coercive and controlling behaviour a crime and finds an online contact form.

Debbie feels safe and secure communicating this way as Steve can't have installed that spyware stuff on it. Debbie writes a message asking what help is available for people who are in a bad relationship and hits send.

A few hours later Steve gets home and after spending a few minutes on the desktop computer flies into a rage. Steve has been able to "sniff" both the web address that Debbie visited earlier and the content of the message that she sent because the police website did not provide a secure-by-default connection.

Steve is so angry at the betrayal that – for the first time – he seriously assaults Debbie. The coercive and controlling relationship is now also a violent one.

- The increasing access to off-the-shelf tools to intercept communications – and the increasing value of the information contained within these communications – means these examples are far closer to reality than many may recognise. Furthermore, the prevalence of such activity can and should be expected to increase in the years ahead.

- While the police are often held to impossible standards, in the context of these examples the police service must take reasonable steps to ensure that their public-facing web infrastructure is as secure as possible.

- It should go without saying that the most determined actor, with sufficient resources, could still engage in activity to intercept secure communications. However, simple steps such as implementing a secure connection can help prevent public safety being undermined – and effective prevention must be recognised as a fundamental of world-class policing and public safety.

Cybersecurity threats are on the rise and, with digital transformation, the police service can expect to be a more appealing target.

- The growth in cybersecurity threats is well-evidenced, both by large-scale data breaches (e.g. TalkTalk, Yahoo and LinkedIn), but also in reports such as Akamai's latest *State of the Internet* security report. It showed that Q2 2016 saw a 129% increase in total Distributed Denial of Service (DDoS) attacks versus the same period a year earlier, with web application attacks up 14% quarter-on-quarter.[5]
- While there is much more to ensuring cybersecurity than simply having a robust and secure SSL/TLS implementation, we have chosen to use the SSL/TLS implementation as a proxy for overall security-mindedness.
- Others have also turned their attention to the issue of SSL/TLS implementation, with Symantec in their most recent *Internet Security Threat Report* declaring that "organisations need to be more proactive around SSL/TLS implementation" emphasising that it is "vital that website managers maintain the integrity of their SSL/TLS implementations".[6]
- Many of the cyber threats facing policing are not unique to policing. Just as wider society and business must ensure they are not complacent to the cyber threat, the police service should also proactively manage and maintain its online infrastructure, especially as it, like other public services, seeks to embrace a digital-by-default strategy in relation to public contact.
- A small number of the sites we examined, including Gloucestershire Police, appeared to utilise DDoS protection. In the case of Gloucestershire, their implementation saw use of a shared (SAN) security certificate. The certificate was found to also be used in relation to 93 other websites, including a South America Bitcoin exchange. Bitcoin is the largely anonymous crypto-currency favoured for use by those either with a deep-seated desire for privacy or with criminal intent.
- The use of a shared certificate can carry additional risks. For example, a force shares a certificate – and real infrastructure, such as a DDoS endpoint – with a Bitcoin exchange. The Bitcoin exchange may be a financially rewarding target and attract significant attack volumes and thus may be more prone to vulnerabilities being identified. Where those vulnerabilities exist in the shared infrastructure, it is easy for an attacker to identify that the police site has the same vulnerability.
- The use of DDoS services does offer the advantage of protection against some forms of attack. However, in utilising a DDoS service the website owner is essentially introducing a man-in-the-middle (MITM) between the web visitor and the police service.
- While the use of encryption is important between the user and the MITM and between the MITM and the underlying web server, it is important to recognise that

[5] *State of the Internet Security Report*, Q2 2016, Akamai

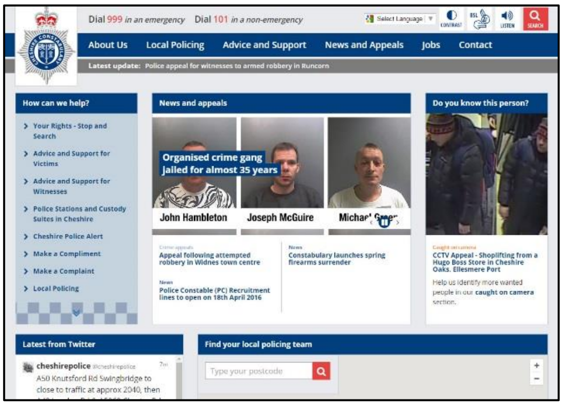
[6] *Internet Security Threat Report*, Volume 21, Symantec, 2016

the MITM (in this case the DDoS service) must at some point decrypt the traffic into plain text and then re-encrypt the traffic.

- This approach is therefore not without risk and it may be worth police forces limiting the use of DDoS services for transactional services where the priority may be the security of communications rather than service availability.
- In any event, the use of DDoS protection services is an area which the National Cyber Security Centre, along with partners, should explore and develop best practice advice as police forces and other public bodies seek to secure and harden their online infrastructure.

Trends in UK policing's public-facing digital infrastructure broadly demonstrate a commitment and ability to deliver security improvements.

- Between July 2016 and September 2016 we noted 11% of sites (8) demonstrated security improvements. These came in the form of adoption of secure-by-default and improving specific implementations.
- However, two sites deteriorated during the period. These were Avon and Somerset Constabulary and Cheshire Constabulary. Further analysis suggests the likely causes of the deterioration.
- While Avon and Somerset's deterioration appears to have been due to a delay in applying a security update, a misconfiguration or other temporary omission, Cheshire's deterioration is a cause for concern.
- Between the first test in July 2016 and the final test in September 2016, the Cheshire site appears to have been upgraded onto a different platform, with a new SSL certificate issued on 26 July 2016. As part of the upgrade the server security configuration has changed, making the implementation less secure, going from a C-grade to an F-grade.



Latest update: Police appeal for witnesses to armed robbery in Runcorn

Your Rights - Stop and Search
Advice and Support for Victims
Advice and Support for Witnesses
Police Stations and Custody Suites in Cheshire
Cheshire Police Alert
Make a Compliment
Make a Complaint
Local Policing

Organised crime gang jailed for almost 35 years

John Hambleton Joseph McGuire Michael Greer

Crime appeals
Appeal following attempted robbery in Widnes town centre

News
Police Constable (PC) Recruitment lines to open on 18th April 2016

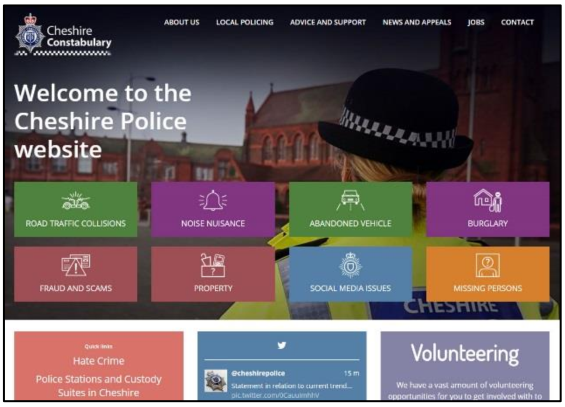
News
Constabulary launches spring firearms surrender

Caught on camera
CCTV Appeal - Shoplifting from a Hugo Boss Store in Cheshire Oaks, Ellesmere Port

Help us identify more wanted people in our caught on camera section.

cheshirepolice @cheshirepolice 7m
A50 Knutsford Rd Swingbridge to close to traffic at approx 2040, then

Old C-graded Cheshire Constabulary Site



Welcome to the Cheshire Police website

Hate Crime
Police Stations and Custody Suites in Cheshire

@cheshirepolice 15 m
Statement in relation to current trend... pic.twitter.com/0CauuImhhV

We have a vast amount of volunteering opportunities for you to get involved with to

New F-graded Cheshire Constabulary site

- The specific failings highlighted in relation to Cheshire's new site include apparent vulnerability to the POODLE attack, support for insecure renegotiation increasing vulnerability to MITM attacks, weak key exchange parameters and no support for the current best protocol (TLS 1.2).

- While a POODLE attack requires a number of pre-conditions, adding to the complexity of launching such an attack, it is concerning that an apparent "upgrade" to public-facing digital infrastructure is in fact accompanied by a deterioration in security.
- Cheshire Constabulary's *Information Technology Strategy 2015-2018* sets out the force approach to information security – "how we secure systems/information". It states that information security will be considered "at the start of all projects/change activity" and "with the Information Security Manager through the life of all project/change activities" in order to "achieve/maintain the required level of security assurance".[7]
- The Cheshire example demonstrates the importance of ensuring that security strategies are put into action and that those charged with information security take their duties seriously and inspect the security of the services they oversee.

Offshoring Data and the Move to the Cloud

It is worth briefly noting that the Home Office's online crime reporting tool (https://report.police.uk) appears to be hosted in the Amazon Web Service cloud using a data centre in the Republic of Ireland, giving some indication of both the progress and the scope for future developments in the UK digital policing infrastructure.

Similarly, Derbyshire Police and South Wales Police both utilise offshored and outsourced A-grade secure forms provided by Wufoo.com, part of the SurveyMonkey group. Wufoo's servers are located in the United States - meaning personal data submitted is transmitted outside of the European Economic Area.[8]

In the wake of the Snowden revelations regarding the ability of US intelligence services to access personal data, the Schrems judgement[9] struck down the Safe Harbor ruling that permitted EU-US data transfer. Any future UK/EU-US privacy arrangements (such as the so-called 'Privacy Shield') could prove pivotal in determining the extent to which UK policing might be able to utilise services hosted outside of the European Economic Area, such as from North America.

While the issue of privacy clearly needs to be addressed where offshoring is concerned, there is also the need to balance privacy concerns with the public

[7] https://www.cheshire.police.uk/media/38810/it-strategy-2015-18.pdf

[8] http://www.wufoo.com/faq/

[9] Schrems v Data Protection Commissioner (Ireland), CJEU, 6 October 2015

interest in ensuring that public safety agencies are able to access an open and effective market for public safety solutions.

If we wish to ensure that world-class services can be developed and/or procured, UK policing should welcome the growing opportunity that exists to obtain cloud-based and other new services from both traditional enterprise suppliers but also, crucially, from new entrants and overseas providers. The National Cyber Security Centre (NCSC) should consider the security implications of public safety services being delivered from data centres outside of the UK.

Recommendations for Securing and Enabling Digital Transformation

- All public-facing UK policing digital infrastructure should move to being secure-by-default. The police service should practice what it seeks to preach and in doing so achieve greater security. It is heartening to see a large and growing number of forces have already moved to a secure-by-default position.[10]
- Forces and organisations should take remedial action to bring their online services to the highest security standards. This action can be easily achieved for the majority of services, involving simple configuration changes to the server. The changes required are achievable by anyone with basic server administration skills.
- Organisations delivering public safety related services should regularly review the security of their platforms. On a basic level this means ensuring in-house teams or outsourced providers are aware of their responsibilities in relation to security and that their services will be subject to security audit by an independent party.
- Contract managers must therefore be familiar with the service that they are overseeing and be willing and able to hold providers to account. Where contracts and agreements make reference to regular security reviews these must be completed and efforts must be made to ensure the independence and integrity of these reviews.
- Similarly, force Data Protection Officers should revisit the College of Policing's Authorised Professional Practice (APP) that sets out their responsibility to oversee "information and systems" and ensure "that security arrangements are in place to protect information" including any "contracts relating to third parties".[11]
- For example, forces, Information Security Managers and their Data Protection Officers should consider the benefits of directly engaging cybersecurity specialists

[10] Territorial police forces with an 'A' grade and secure-by-default: Cleveland, Cumbria, Devon and Cornwall, Dorset, Durham, Gwent, Kent, Leicestershire, Merseyside, Norfolk, North Yorkshire, PSNI, Suffolk, Warwickshire, West Mercia and West Yorkshire.

[11] https://www.app.college.police.uk/app-content/information-management/data-protection/

- independent of their IT suppliers/providers - to conduct security reviews and audits. This will help ensure a robust and rigorous independent process exists.

- As forces and public safety agencies – like Cheshire Constabulary – overhaul and deploy new public-facing digital services the project lead, Project Owner or Senior Responsible Owner (SRO) must ensure due care and attention is paid to the security of the digital infrastructure to avoid increasing vulnerability to exploitation at a time of rising threat.
- With ever increasing reliance on digital services in and around policing it is important that mechanisms are also made available to allow specific cyber security issues or vulnerabilities to be reported in a safe and secure manner.
- The United States Computer Emergency Readiness Team (US CERT) has a reporting form through which issues can be identified.[12] At present no such readily identifiable and open mechanism exists for the UK's public services.
- The imminent launch of the UK's National Cyber Security Centre (NCSC) provides an opportunity to remedy this.[13] While the NCSC "will not offer an enquiries line for the general public", we believe it would be a grave mistake for the NCSC not to afford an open and publicly accessible means of reporting cyber security threats or vulnerabilities affecting the UK's public services.
- At present the NCSC offers a 'Cyber-security Information Sharing Partnership' allowing industry and government to exchange cyber threat information in real time – however the facility is only open to organisations sponsored by a government department, existing CiSP member or trade body/association.
- NCSC should consider the lessons from the British experience of successful counter-terrorism efforts and apply these in the context of threats to cybersecurity. This means having a public-facing and readily accessible mechanism for individuals or organisations not eligible for CiSP membership to submit reports or concerns in a timely fashion.
- In turn the National Police Chiefs' Council should ensure there is an appropriate mechanism in place to handle and manage any submissions or referrals that relate to services operated by or on behalf of UK policing.
- Senior officers regularly rely on the advice of tactical advisers in specific situations. The same needs to be accepted in digital transformation. To truly secure the maximum benefit from technology, UK policing needs to look beyond the usual suspects to identify and recruit the most talented and enterprising digital and technology professionals.

[12] https://www.us-cert.gov/forms/report

[13] https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus

- In particular, UK policing should consider the merits of greater collaboration with the Government Digital Service and the development of new mechanisms by which the service can attract some of the best talent and avoid some of the costliest mistakes of the past. As importantly, an injection of fresh and disruptive talent in policing would help drive a compelling digital vision for both the police workforce and the public they serve.[14]

Organisations with the Highest Gradings

Organisations that achieved the best - world-class - ratings provide secure connections by default, which is increasingly the norm online and an indicator of taking security seriously. The achievement by the Government Digital Service (GDS) in the case of GOV.UK (on behalf of the Civil Nuclear Constabulary) and the Independent Police Complaints Commission (IPCC) demonstrates that an A+ grade can be achieved in public services. We also tested our own performance – receiving an A+ grade – demonstrating that the standard and practice of world-class secure connections are not the preserve of organisations with large budgets. The progress of the constabularies of Norfolk and Suffolk is considered noteworthy.

Organisation	Grading	Notes
The Centre for Public Safety	A+	Secure-by-default.
Civil Nuclear Constabulary (CNC)	A+	Secure-by-default. Hosted on GOV.UK, developed and operated by the GDS[15].
Independent Police Complaints Commission (IPCC)	A+	Secure-by-default.
Cleveland	A	Secure-by-default.
Cumbria	A	Secure-by-default.
Devon and Cornwall	A	Secure-by-default.
Dorset	A	Secure-by-default.
Durham	A	Secure-by-default.
Gwent	A	Secure-by-default.
Kent	A	Secure-by-default.
Leicestershire	A	Secure-by-default.
Merseyside	A	Secure-by-default.
Norfolk	A	Secure-by-default. Graded F in July 2016.

[14] The Centre for Public Safety will be seeking to progress work on this theme in the year ahead.

[15] Government Digital Service - https://gds.blog.gov.uk/about/

North Yorkshire	A	Secure-by-default.
Police Service of Northern Ireland (PSNI)	A	Secure-by-default.
Suffolk	A	Secure-by-default. Graded F in July 2016.
Warwickshire	A	Secure-by-default.
West Mercia	A	Secure-by-default.
West Yorkshire	A	Secure-by-default. Graded U in July 2016.[16]

Organisations with Room for Improvement

A number of organisations scored well but failed to make use of secure-by-default or otherwise missed out on the highest grades.

Organisation	Grading	Notes
ActionFraud (1 of 2)	A-	Version for reporting financial loss.
Bedfordshire	A-	Specific tri-force solution.
Cambridgeshire	A-	Specific tri-force solution.
Gloucestershire	A-	Main site graded A, previously in July 2016 was graded C. Downgraded to A- as certificate is shared with other domains unconnected to UK policing.
Hertfordshire	A-	Specific tri-force solution.
NCA SAR Online	A-	National Crime Agency Suspicious Activity Reports Online. Graded C in July 2016.
South Yorkshire	A-	Secure-by-default for online services only.

This makes a total of twenty-six sites graded A- or better (allowing for our adjustments). The Trustworthy Internet Movement's *SSL Pulse* considers these to be 'secure sites' while it defines the remaining 45 sites as having 'inadequate' security.[17]

Organisations with Significant Room for Improvement

A number of organisations were identified with significant room for improvement. These included a number of forces - both large and small - along with elements of the Home Office, the College of Policing's NCALT service, the NPCC's Criminal Records Office, ActionFraud (for reporting phishing and malware) and CrimeStoppers.

[16] http://www.westyorkshire.police.uk/asbform

[17] https://www.trustworthyinternet.org/ssl-pulse/

A number of organisations have been specifically downgraded (marked with *) from 'A' grades as they failed to fully implement secure connections for forms on their site or had mixed content issues.

Organisation	Grading	Notes
ACRO	B	Criminal Records Office run by the National Police Chiefs Council (NPCC).
City of London	B	Graded F in July 2016.
CrimeStoppers UK	B	
Derbyshire	B*	Main site offers no inherent SSL but uses outsourced A-graded iframe forms hosted in the United States.
Her Majesty's Inspectorate of Constabulary (HMIC)	B	
Home Office Terrorism Tool	B	Reporting Terrorist and Harmful Extremist Material Online tool.
Home Office Reporting Tool	B	
Northamptonshire	B*	Partial implementation of 'A' grade SSL.
Police Ombudsman for Northern Ireland	B	
Police Scotland	B*	Partial implementation of 'A' grade SSL.
Track My Crime Tool	B	Used by a number of forces.
West Midlands	B*	Mixed content issues with 'A' grade SSL.
Wiltshire	B*	Partial implementation of 'A' grade SSL.
ActionFraud (2 of 2)	C	Reporting tool for phishing and malware.
Avon and Somerset	C	Graded A in July 2016.
Lincolnshire	C	
Metropolitan Police	C	
National Driver Offender Retraining Scheme (NDORS)	C	Individual NDORS online boking sites requesting personal data were found to range from grade A to grade C.[18]
NCALT (College of Policing)	C	Police e-learning environment.
Nottinghamshire	C	Graded U in July 2016.
True Vision Hate Crime Tool	C	Hate crime reporting tool.

[18] In addition to the main NDORS site we also tested a number of online booking services provided for different areas and courses. These sites ranged in score from grade A to grade C.

Organisations with Significant Vulnerabilities

The table below lists those sites which were graded F as part of the scans. These were primarily due to failings to fix well-documented weaknesses in secure encryption or the use of insecure protocols and cipher suites.

Organisation	Grading	Notes
CEOP	F	Child Exploitation and Online Protection Centre is part of the National Crime Agency (NCA).
Cheshire	F	Cheshire previously scored a C in July 2016.
Essex	F	Portions of site utilise A-graded SSL, while others - especially the transactional elements - utilise F-grade SSL.
Lancashire	F	SSL only for online services microsite.
South Wales	F	Graded F in relation to their e-services with the main site having no SSL, except for the use of outsourced A-graded forms hosted in the United States.
Staffordshire	F	Site states "Staffordshire Police is taking Cyber Crime very seriously."[19]
Thames Valley	F	

Organisations with No Secure Connection

A total of 17 organisations either provided no automatic secure connection for the transfer of personal data or else failed to provide any form of secure connection at all.

More than 70% (12) of these organisations offered users the ability to submit personal data - and in some cases information relating to criminal activity and suspects - over plain text. These organisations are placing members of the public at unnecessary risk.

The cost of an A+ graded SSL connection is insignificant to these organisations, so the failure to deliver a secure connection is therefore due either to a judgement that the risk is acceptable, or a lack of awareness of the risk in the first place.

These organisations should as a matter of priority implement secure connections. The Centre for Public Safety is of the view that there is no valid reason why any of these organisations cannot achieve A+ grading by the time we revisit the issue of cybersecurity in 2017.

[19] https://www.staffordshire.police.uk/cybercrime

Organisation	Grading	Notes
British Transport Police	U	Personal data over plain text.[20]
College of Policing	U	No personal data identified.
Dyfed-Powys	U	Personal data over plain text.[21]
Greater Manchester	U	Personal data over plain text.[22]
Hampshire	U	Personal data over plain text.[23]
Her Majesty's Inspectorate of Constabulary in Scotland (HMICS)	U	Personal data over plain text.[24]
Humberside	U	Personal data over plain text.[25]
Ministry of Defence Police	U	No personal data identified.
National Crime Agency	U	No personal data identified.
National Police Air Service	U	No personal data identified.
National Police Chiefs' Council	U	No personal data identified.
North Wales	U	Personal data over plain text.[26]
Northumbria	U*	Downgraded from A grade as personal data transmitted over plain text by default.[27]
Police Investigations and Review Commissioner (PIRC)	U	Personal data over plain text.[28]
Surrey	U*	Downgraded from A- grade as personal data transmitted over plain text by default.[29]
Sussex	U*	Downgraded from A- grade as personal data transmitted over plain text by default and certificate is untrusted/expired.[30]
UK Missing Persons Bureau	U	Personal data over plain text.[31]

[20] http://www.btp.police.uk/contact_us/general_enquiries.aspx

[21] http://www.dyfed-powys.police.uk/en/contact-us/report-online/

[22] http://www.gmp.police.uk/content/feedbackintelligence.html?openform

[23] http://www.hampshire.police.uk/internet/do-it-online/online-forms/request-call-back.html

[24] http://www.hmics.org/contact-us

[25] http://www.humberside.police.uk/signup-for-updates

[26] http://www.north-wales.police.uk/contact/minor-incident-reporting-new.aspx

[27] http://www.northumbria.police.uk/101form

[28] http://pirc.scotland.gov.uk/how_to_request_a_review/review_form

[29] http://www.surrey.police.uk/contact-us/

[30] http://www.sussex.police.uk/contact-us/report-online/report-a-crime/report-personal-crime-domestic-abuse-hate-crime-and-sexual-offences/

[31] http://missingpersons.police.uk/en/case/15-007500

Methodology

The sites were collated and examined to see if they supported SSL technology. Where no automatic support was found a process was conducted to identify any specific SSL-enabled forms, microsites or pages. In addition, a number of non-police SSL-enabled sites were identified during the scanning and where these had a connection to public safety or law enforcement they were also included in the tests.

Tests were all conducted on 7 July 2016 and repeated again on 28 September 2016 and utilised a public and free-to-use Qualys® SSL Labs' SSL Service in accordance with their terms of use. A small number of sites were scanned using an alternative SSL checking service owing to apparent blacklisting of the primary service in July 2016. A consistent scoring method was applied in order to ensure comparability.

Grading Overview

The table below provides an overview of how the grading system works. You can read more in the *SSL Server Rating Guide*.[32] Where an organisation has multiple SSL implementations then we use the lowest grade. We have made a number of additional adjustments in response to other concerns regarding the implementation, as detailed in the grading tables above.

Grade	Example of Exploits or Issues at each Grade
A+	• Exceptional configuration, incorporating HSTS and no warnings.
A	• The server scores at least 80% and supports TLS 1.2.
A-	• The server scores at least 80% but does not support Forward Secrecy.
B	• The server scores 65-79% and/or the server accepts the RC4 cipher or support weak Diffie-Hellman key exchange.
C	• The server scores 50-64% and/or the server may be vulnerable to the POODLE attack and use older protocols.
D	• The server scores 35-49% on key measures.
E	• The server scores 20-34% on key measures.
F	• The server scores less than 20% and/or supports insecure anonymous cipher suites.
U	• No secure connection to grade - or the connection only accessible by forcing a connection manually. Where this is the case the grading for the secure connection is also provided. The worst performers are those graded U, accepting personal data.

[32] https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf

The Centre for Public Safety

About the Centre for Public Safety

The Centre for Public Safety seeks to support frontline professionals and to advocate for world-class policing and public safety through a focus on research, action, leadership and events. Founded in 2016 and based in the United Kingdom, the Centre looks within and beyond the shores of the British Isles in a deliberate bid to identify examples of world-class public safety.

For more information you can contact the Centre via contact@centreforpublicsafety.com or visit the Centre's website at https://www.centreforpublicsafety.com.

🐦 @CenPublicSafety

About the Author

Rory Geoghegan is the Director of the Centre for Public Safety. After three years as a frontline police officer in the London Borough of Lambeth, spending the majority of his time as a Dedicated Ward Officer, Rory founded the Centre for Public Safety. Before joining the Metropolitan Police, Rory was a Crime & Justice Research Fellow at Policy Exchange, making regular media appearances and authoring *The Future of Corrections*, *Inside Job* and *Cost of the Cops*. Prior to this he worked as a senior researcher on transformational change at the Institute for Government and as a commercial and strategy consultant in financial services at PricewaterhouseCoopers. Rory read Philosophy, Politics and Economics at Trinity College, Oxford.

🐦 @RoryGeo

Published by The Centre for Public Safety

9 781912 028696 >

Copyright © The Centre for Public Safety 2016
4th Floor, 86-90 Paul Street, London EC2A 4NE, UK
centreforpublicsafety.com
ISBN: 978-1-912028-69-6