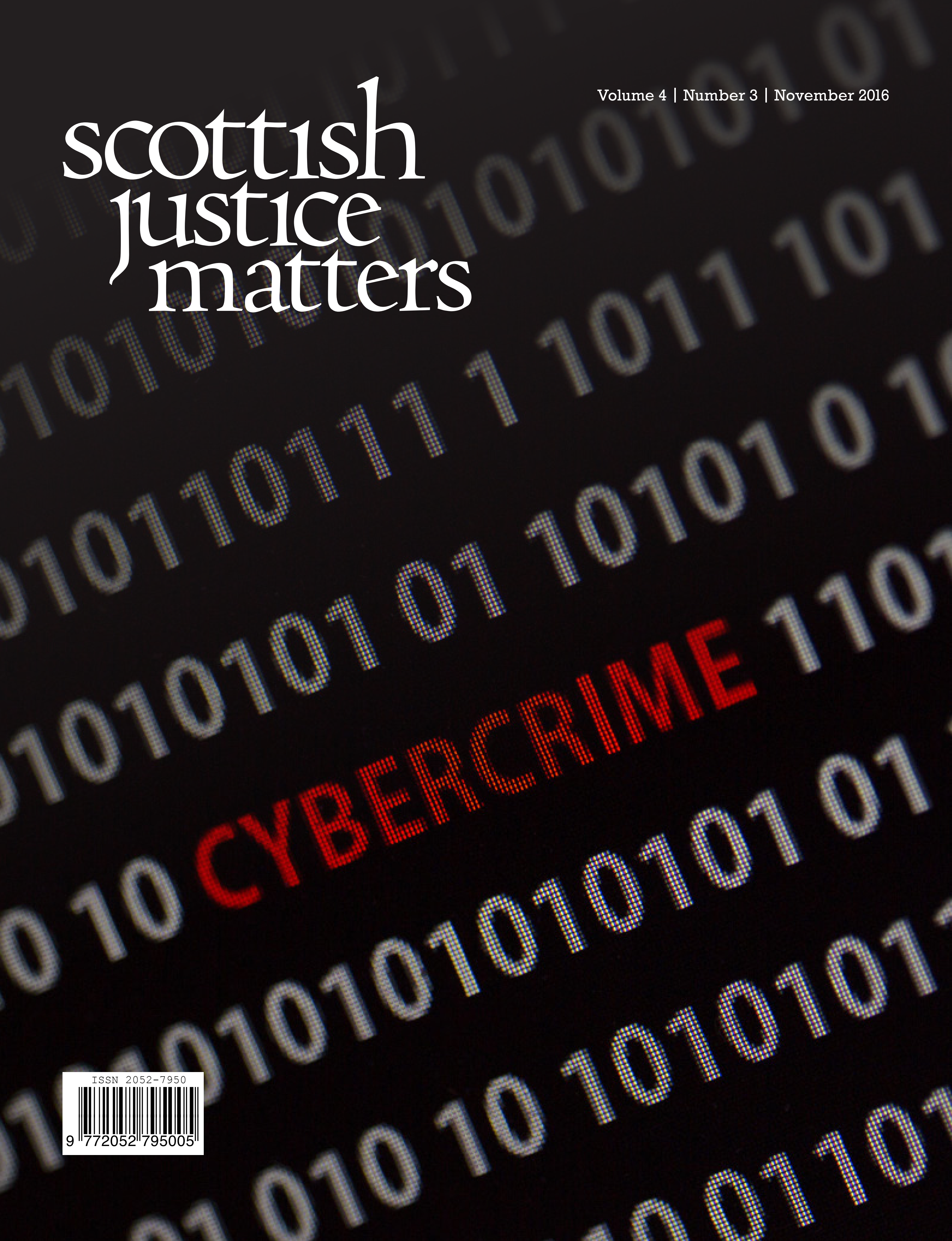
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950
9 772052 795005

ETHICAL HACKING

Rory McCune on the Rise and Fall (?) of Penetration Testing

PENETRATION TESTING (a.k.a ethical hacking or security testing) has been a growth industry for some time now. From humble beginnings with small boutique security companies with a handful of dedicated testers, the UK now has large providers with several hundred dedicated penetration testing consultants. However, despite this growth, we are now seeing companies turning to alternate sources for finding security bugs in their software and systems, which may supplement or even supplant traditional testing approaches.

What is Penetration Testing?

The penetration testing industry is a relatively young one which has grown up alongside the Internet and specifically around E-Commerce.

The idea behind penetration testing is to take a 'hacker's eye' view of a system and attempt to bypass security controls to gain unauthorised access to the system. In the early days this largely focused on attempts to compromise server systems and web sites, but now there are a huge range of systems which are subjected to this kind of testing; from phones and tablets, to "Internet of Things" devices, to cars. However, regardless of this widening of the range of devices targeted, the basic approach of emulating an attacker has stayed fairly constant.

This approach does however have a limitation, which is that penetration testers can't actually emulate attackers, if the attack would be illegal to complete despite the authorisation of the system owner. Modern attackers have an array of techniques at their disposal such as buying "0-day" exploits for security vulnerabilities that have no fix from the vendor on "Dark Web" marketplaces; and targeting associated companies and personal or home computers of staff members of their targets directly.

The growth of Penetration Testing as a service

Initially, the main customers for dedicated security testing companies were large financial services organisations, together with some government departments which dealt with sensitive or 'secret' information.

Penetration testing was seen as part of the security process for these high-value systems, with reviews being completed before the system went live and then annual reviews being completed to test that they were still sufficiently secure.

This meant that there were a relatively small number of niche providers in the UK serving this market. Over the last 15 years we have seen substantial growth in this marketplace. Today the largest penetration testing company in the UK (NCC Group PLC) has over 250 UK based dedicated penetration testing consultants, and there are 65 companies registered to provide penetration testing services in the main industry body, the Council for Registered Ethical Security Testers (CREST) (www.crest-approved.org/uk/members/index.html).

Also changed is the variety of companies who make use of penetration testing services. With the ever-increasing level of use of IT, customers are no longer restricted to central government and financial services. A modern security testing company can expect to do business with every business sector from retail organisations to charities, from start-ups to major banks.

One of the main drivers for the increasing use of penetration testing services has been the Payment Card Industry Data Security Standard, which mandates that companies processing payment card information have regular security testing. This is a rare piece of regulation where specific technical measures were required and is one of the few that specifically insists on penetration testing as a requirement (see: www.pcisecuritystandards.org/).

The growth in penetration testing has also been driven by a marked shift in the online threat environment. It is fair to say that there has been a huge increase in the number of security breaches suffered by companies. A week rarely passes without us hearing about another breach, and now 'breach fatigue' has set in to the degree that only really large breaches, like the recently announced Yahoo incident (Yahoo 22.9.16) consistently appear in mainstream media.

In addition, criminals have been becoming markedly more advanced in their attacks. Modern 'cyber criminals' have shown evidence of high levels of technical aptitude and the facility to string together expertise in different areas of information technology to achieve their goals.

In the face of this changing threat, there have been some questions raised about whether traditional penetration testing alone can provide companies with all the assurance that they need. When security tests are conducted, they are usually done with a firm scope in mind and a number of days assigned to complete the assignment. Consultants are careful to avoid 'off-scope' testing as there are concerns that this could fall foul of Computer Misuse Act 1990 clauses relating to unauthorised access to systems.

Unfortunately, attackers rarely concern themselves with these kind of limitations and in many cases they are able to take advantage of this to target peripheral systems which may not be within the scope of normal penetration testing.

The rise of Bug Bounties

This perceived gap in testing methods has led the rise of "Bug Bounty" programmes, where companies pay independent researchers for security vulnerabilities which they find in their systems. Whilst the concept of bug bounties has been around since the 1990s it has only been in the last 5-6 years that they have really taken off, with companies like Google and Facebook leading the charge.

These programmes partially stemmed from the activities of 'white hat' hackers who would find security vulnerabilities in third party sites and report them. Unfortunately, these activities fall into a very grey area of the law as they involve the researcher probing systems to some degree while looking for issues. Over the last 15 years this has led to a number of cases where potentially well intentioned researchers have been threatened by companies whose products they were researching, with the intention of restricting access to the information about discovered vulnerabilities.

Bug bounty programmes formalise the engagement process between researchers and target companies, which helps provide comfort to potential bug hunters that they won't be sued for their efforts and also lets companies specify what areas they are, and are not, happy to have tested.

The approach used in bug bounty programmes is markedly different from traditional testing. There is no vetting of the people carrying out the work and no contract in place between the target company and the researcher finding the issue. Instead, companies rely on a defined scope of what systems and networks are considered as generally 'available' for exploitation, and additionally, what kinds of issues will trigger pay-outs.

The amount paid varies extremely widely from company to company. Many providers only provide recognition of the bug which has been found and perhaps 'swag' consisting of T-shirts or other branded company merchandise. At the other end of the scale are companies like Google who recently announced that they would pay up to $200,000 for successful attacks on their Android operating system (https://googleprojectzero.blogspot.co.uk/2016/09/announcing-project-zero-prize.html).

With such large quantities of money on offer, it's unsurprising that bug bounties have seen substantial take-up. Of course popularity is not without its drawbacks, and there have been quite a large number of complaints of low quality submissions and researchers being aggrieved when told that their submission does not qualify for a suitable pay-out.

Additionally, the process of administering these programmes can be quite onerous, and this has led to a rise of middle-men companies, such as Bugcrowd and Hackerone who offer help in setting up and running these programmes for other organizations.

The downfall of Penetration Testing?

This rise of this alternate approach to security has led some to suggest that it will replace penetration testing. Obviously, only having to pay for exploitable issues as opposed to paying regardless of what is found can prima facie seem attractive, especially to companies with many systems that need to be reviewed.

However, it is clear that bug bounties have some fairly serious limitations. The most significant of these is that they essentially give consent for unvetted individuals to attack a company's systems. Whilst this may be acceptable for Internet facing systems which are open to attack anyway, most companies would draw the line at either opening up their internal systems for access or providing credentials to critical systems to allow for the kind of authenticated penetration testing that is a common occurrence for many organizational types.

In addition, administering a bug bounty programme requires a level of security knowledge internally in assessing findings, and externally in responding to participants which are less likely to suit smaller companies.

The future of Penetration Testing

Over the last 15 years, penetration testing has evolved from being a relatively small niche service to one that is used by most large organisations in one guise or another. Looking ahead, it would seem that more growth is inevitable as companies and the public sector drive more and more of their operations into the cyber realm and the vulnerabilities in those services continue to be exploited by varying attacker groups. Additional approaches to finding security flaws, like bug bounties, are likely to remain complementary to penetration testing and both of the approaches will need to be utilized to their fullest extent if the increasing tide of security breaches is to be stemmed.

Rory McCune is a managing consultant at NCC Group PLC and has worked in a variety of IT and Information Security roles, specialising in penetration testing and application security.

rory.mccune@nccgroup.trust

Yahoo (22.9.16) yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security