Dark Clouds on the Horizon

The Challenge of Cloud Forensics

Ian Ferguson & Karen Renaud
Division of Cybersecurity
Abertay University
Dundee, Scotland, DD1 IHG
Email: {i.ferguson,k.renaud}@abertay.ac.uk

Alastair Irons
Faculty of Computer Science
University of Sunderland
Sunderland, United Kingdom, SR1 3SD
Email: alastair.irons@sunderland.ac.uk

***Abstract*—We introduce the challenges to digital forensics introduced by the advent and adoption of technologies, such as encryption, secure networking, secure processors and anonymous routing. All potentially render current approaches to digital forensic investigation unusable. We explain how the Cloud, due to its global distribution and multi-jurisdictional nature, exacerbates these challenges. The latest developments in the computing milieu threaten a complete "evidence blackout" with severe implications for the detection, investigation and prosecution of cybercrime. In this paper, we review the current landscape of cloud-based forensics investigations. We posit a number of potential solutions. Cloud forensic difficulties can only be addressed if we acknowledge its socio-technological nature, and design solutions that address both human and technological dimensions. No firm conclusion is drawn; rather the objective is to present a position paper, which will stimulate debate in the area and move the discipline of digital cloud forensics forward. Thus, the paper concludes with an invitation to further informed debate on this issue.**

Keywords–Cloud Forensics; Challenges

I. INTRODUCTION

The seeds of Cloud Computing were sown back in 1963 when Licklider talked about an "*intergalactic computer network*" [1]. He had a vision of a global network allowing people to execute code anywhere and access data anywhere. The world had to wait for the capacity of the Internet before this dream would come to fruition. In 1999, Salesforce delivered services to Enterprise via a website [2]. Soon large companies, such as Amazon and Microsoft, started to offer enterprise and personal computing services. Many organisations now use Microsoft's Office 365 platform to manage their email and store their documents. Licklider's dream has been realised.

Cloud computing offers obvious benefits to companies and individuals [3]. The costs are reasonable, as compared to investing in, and maintaining, their own infrastructure.

Yet there is a flip side too, related to those who use computing power for nefarious purposes. When law enforcement officials investigate crimes it is common practice for them to seize devices for analysis by forensics experts.

Digital forensics, as a science, emerged as cyber crime started to increase, and did so to meet the needs of law enforcement and also to help organisations to reveal the activities of cyber attackers. Rigorous forensics procedures emerged and were adopted by forensics investigators [4]. The advent of the cloud challenges these established procedures, adding a whole new dimension of complexity to forensics investigations. Challenges come from technical, stakeholder, organisational and political levels.

In this paper, we discuss the challenges experienced by the humans involved in usual and cloud forensics investigations [5].

Options for a digital forensic response to the emergent challenges are discussed in the hope of provoking discussion on a response that is grounded not solely in technology but rather one that is multi-disciplinary incorporating elements from various stakeholders in the criminal justice process (law makers, law enforcement) and society at large.

We commence by discussing the progress of technology and introducing forensics in Section II. We then introduce the concept of cloud computing in Section III. We continue our discussion by advancing the argument that progress, in the shape of security technology, may lead to a situation in which information only exists "in the clear" (i.e., unencrypted) as it is input and output (Sections IV and V). All storage and computation will be performed upon a provably securely encrypted representation, resulting in an encryption boundary encircling all data.

We contemplate the concept of a "robust" system and discuss how such a system might arise from the encryption boundary. The consequences for the digital forensics community of the existence of such a system are examined. We also address the concept of the cloud and its impact on digital forensics.

We then discuss existing responses to individual threats in Section VI. Consideration is given to the combined threat and to the technical, legal and ethical aspects of the problem including community roles and attitudes to the problem, taking into account the need to maintain evidential integrity and continuity. Some possible digital forensic responses are discussed, including their technical feasibility, ethical desirability and current admissibility in Section VII. Section VIII concludes by inviting debate on the technical, ethical and legal consequences of the various response options.

II. TECHNOLOGY, PROGRESS & FORENSICS

An ethical paradox lies at the heart of all security research: one that presents a problem to the digital forensics community. The more secure we make things, the less we can get into them when we need to. It is possible that the ordinary security researcher does not worry too much about this on a day-to-day

 ISBN: 978-1-61208-607-1

basis. Happy with the assumption that they are on the side of the "good guys", and that their job is to keep the "bad guys" out, they continue to develop ever stronger encryption, more user-friendly security systems and generally, with a defenders mindset, build ever higher digital castle walls.

One specific kind of researcher, namely the digital forensic scientist, is likely to regard these fortifications with trepidation. The obvious question is: *"What happens if the 'bad guys' have seen how we secure our "valuables" and use the same measures?"*

Since Kerckhoff's principle [6] mandates that the "protection plans" should be in the public domain, we must assume that the bad guys will have access to, and employ, the same technology as the good guys.

Current digital forensic techniques can, to some extent, be said to work by accident. It is only because the normal functioning of hardware, operating systems and applications leave artefacts lying around that the reconstruction of user activity is possible. Less sophisticated cyber criminals might still leave sufficient cybertrails at the scene of the cybercrime. Garfinkel [7] has argued that we have been living in a "golden age" of digital forensics. To date, these artefacts and the inevitable human fallibility in implementing "secure" systems have meant that the digital forensic investigator has been able to sneak into the digital storage mechanism and look around.

However, cyber security, and its uptake by criminal elements, will inevitably challenge forensics investigators. The consequences of this may include an "evidence blackout." How we could respond to this is the subject of this paper.

It could be argued that we do not need to worry about this yet. It might be the case that human fallibility will always defeat attempts to make systems secure. However, improving security seems to be the *raison d'être* of the larger security research community and their techniques will inevitably be embraced by criminal elements.

The literature on digital security often identifies the human as the weakest point in any digital security system. What happens if this is reversed and the human, in this case the cyber criminal, becomes the strongest link? How will greater awareness of the strengths and weaknesses of digital investigations help cyber criminals to obfuscate their cybertrails? Recent cases have suggested that this era might well have dawned. Two examples demonstrate this. The first is the San Bernadino case [8] where the US government attempted to force Apple to help them to access data on iPhones. The second is that in the days following the Texas church shooting the FBI complained about not being able to access the shooter's phone [9]. These are evidence of a significant phase change: a new challenge for law enforcement.

There are also signs from Western governments that the use of encryption by subversives is making counter-terrorism efforts challenging [10], [11], [12], [13].

III. Cloud Computing

The term "Cloud Computing" has various overloaded meanings conventionally categorised as "software as service", "platform as service", "infrastructure as service" etc., and is a growing area of interest in the digital investigation community [14].

Cloud forensics can be defined as *"a hybrid forensics approach (e.g., remote, virtual network, live, large-scale, thin-client, thick client) towards the generation of digital evidence"* [15].

One particular feature of some cloud computing systems likely to prove troublesome to forensic investigators is the idea of the distributed, fragmented file system. Originally conceived partly for reasons of data security and mapping easily onto the cloud paradigm, it has its origins in the work of Shamir [16] and Rabin [17], with implementations such as OceanStore [18], PASIS [19] and more recently the work of Mei *et al.* [20]. Such systems achieve security by storing a file not on one remote networked file server but by splitting a file into fragments and storing each fragment on (potentially geographically separate) servers.

The underlying idea is that if one server is attacked and compromised, then the attackers still do not have access to a file — that requires the more difficult proposition of compromising all the servers across which the file is stored. Couple this with full disk encryption, with each fragment protected by a different key, and we have a perfect storm. Anyone wishing to reconstruct a file is thus potentially faced with the theoretical problem of decrypting multiple encryption regimes and also the practical problems associated with data fragments existing in multiple jurisdictions, and possibly even the knowledge of the file fragments' locations being likewise encrypted and distributed.

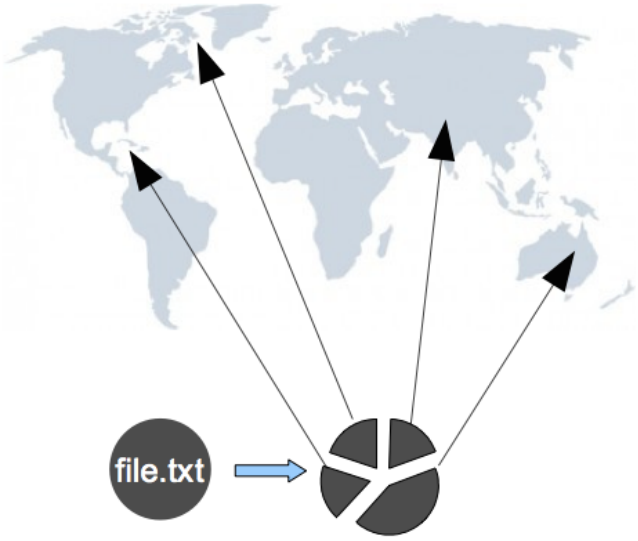

Figure 1. Fragmented file storage in the cloud computing paradigm

In an Internet-wide cloud context, different parts of the same file will be in different computers, different countries and different jurisdictions (See Figure 1). The practical difficulties of obtaining the file are thus indeed daunting. Uptake of the cloud computing paradigm is widespread [21].

IV. Individual Technical Threats

In this section, a number of security technologies that may threaten an "evidence blackout" are individually examined before we discuss the consequences of deploying them

 ISBN: 978-1-61208-607-1

together. The techniques/technologies considered are: full disk encryption, secure network communication, secure processors, homomorphic encryption and anonymous routing.

A. Encryption

It is worth briefly examining the state of the art of encryption technology and its adoption.

Current encryption techniques are based on the idea of computational security. Given encryption keys of sufficient length, cryptanalysis requires infeasible amounts of computing power and/or lengths of time. The existence of techniques and/or computing power able to tackle current cyphers in a meaningful time-scale is not acknowledged by those likely to possess them. Encryption has thus reached the point of being "practically unbreakable".

B. Full Disk Encryption (FDE)

Current digital forensic techniques depend largely on artefacts left behind on disk, both explicitly, and as a by-product by the operating system. The first "dark cloud" on the horizon is that these techniques do not perform well when faced with serious attempts at concealment by encrypting full disks [22].

Full disk encryption allows the entire contents of a disk to be protected by a password/key scheme, i.e., no-one without the key (digital investigators included) can read the contents of the disk. To achieve this, a layer is introduced into the Operating System between the file system and storage media device driver. Any data being written to the disk is encrypted on-the-fly as it passes through this layer. Conversely, any data being read is decrypted, provided that the correct decryption key has been provided at the beginning of a session.

The advantage of such a scheme is that it is largely transparent to the user — no special actions are required to conceal particular items of data as *everything* is automatically encrypted/decrypted. Popular implementations of this technology include VeraCrypt [23] and Bitlocker [24].

C. Secure network communication

The transmission of strongly encrypted messages, once the province of governments, military and intelligence services is within the grasp of both the ordinary citizen, and the criminal. HTTP Secure (HTTPS), Virtual Private Network (VPN), Internet Protocol Security (IPSec) and all have achieved widespread adoption.

D. Secure Processors

Secure processor technology promises to do for memory image forensics what full disk encryption did for disk examination — i.e., render it impossible. In a system with a secure processor, all data outside the boundary of the processor itself i.e., anything in random access memory (RAM), is encrypted. Both program instructions and data are decrypted on-the-fly with block ciphers as data is shifted to and from the various system buses (See Figure 2).

Having their origins in systems such as Aegis [25] and Bastion [26], secure processors were originally intended to provide a secure environment for embedded control systems but continue to develop towards high-end systems. Although they are not yet widely adopted in desktop level systems (mainly due to speed issues in dealing with the large cryptographic overhead) working systems are emerging.

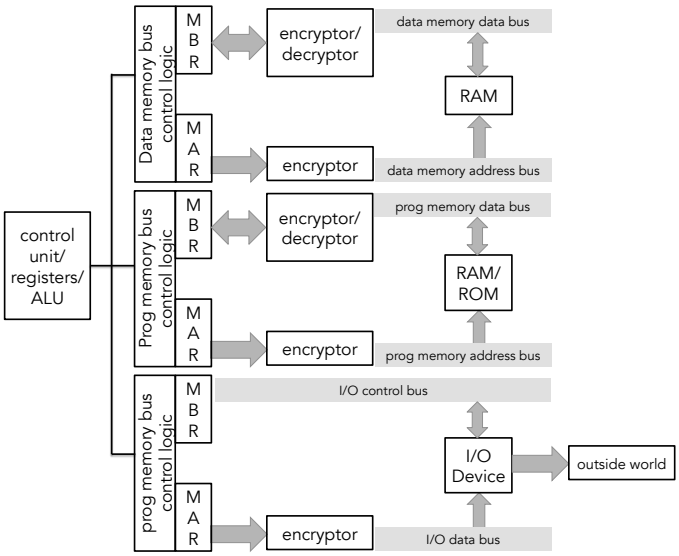

Figure 2. Secure Processor Architecture (MBR=Master Boot Record; MAR=Memory Address Register; ALU=Arithmetic Logic Unit)

E. Homomorphic Encryption

Homomorphic encryption (HE) is the idea that computation can be performed directly on the encrypted representation of data without the need first to decrypt it. First proposed by Rivest *et al.* [27] it would enable data not only to be stored securely in the cloud, but also to be processed there without fear of compromise by a corrupt cloud service provider.

The work of Gentry [28], based on ideal lattice cryptography, has shown that such a scheme is viable, but currently the computational overhead involved means that it is not yet practical. Efforts to discover a more computationally tractable scheme continue [29].

F. Anonymous Routing

Due to the nature of the protocols underlying the operation of the Internet, it is possible to identify the source and destination of network traffic. Even if encryption is in place, it is thus possible to establish that two parties are in communication.

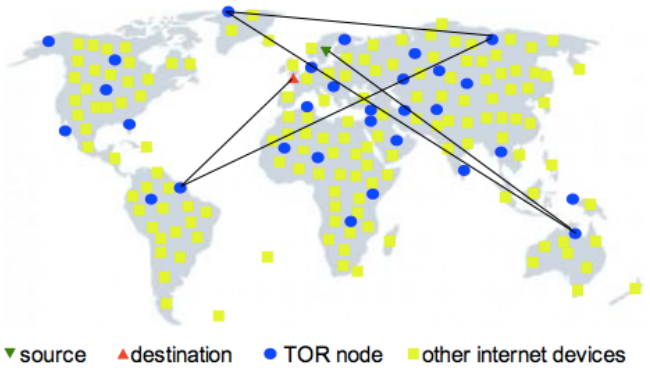

Figure 3. Onion Routing

The advent of anonymous routing (e.g., onion routing as embodied in the The Onion Router (TOR) protocol [30])

 ISBN: 978-1-61208-607-1

removes this source of evidence. The TOR works by separating the concerns of identity and routing. It forwards messages randomly though a network of TOR servers (nodes), with each one applying a layer of encryption (hence the onion metaphor) before forwarding the packet to the next node or ultimately its intended destination. This prevents both the source and destination of the message from being known by every node and prevents traffic analysis (See Figure 3).

Whilst current onion routing implementations have their weaknesses (various attacks against the anonymity have been demonstrated), systems such as the TOR network have demonstrated their viability. Such techniques are available to those with sufficient knowledge and reason to hide the origin and destination of their incoming and outgoing data.

V. The Combination of Threats

Although the threat of encryption has been identified previously in work such as that of Garfinkel [7] and Seigfried *et al.* [31], digital forensics has thus far managed to keep evidence flowing by reducing reliance on the initial acquisition strategy of imaging cold systems and resorting to live imaging/live forensics. How well this approach would scale should the need for it become widespread remains to be seen.

Due to the threats outlined in the previous section it is possible to envisage a computing system in which the only place that data exists "in the clear" (i.e., in unencrypted form) is internally in the processor, during input (mouse, keyboard events, etc.) and when formatted for human consumption i.e., display/rendering (and hence the video RAM, audio and printer buffer etc.). Anything stored in either primary or backing store, or in transit over a communication channel is likely to be strongly encrypted. Thanks to the cloud, homomorphic encryption and anonymous routing threats, not only will any evidence be encrypted, it will also be difficult to find which machine it is on or even where it is physically located. This would lead to an "evidence blackout" as current approaches to investigation (largely based on disk and RAM images) will fail.

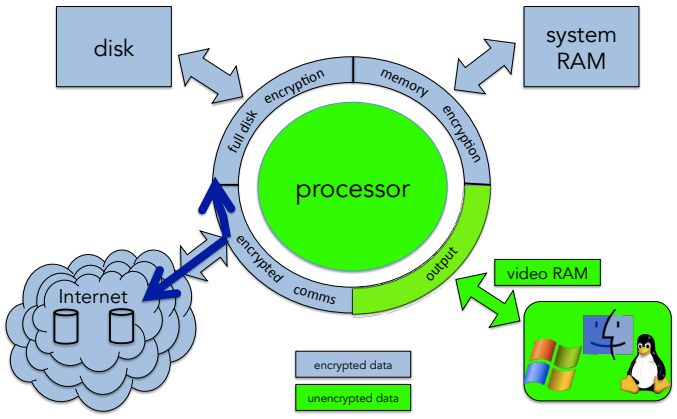

Figure 4. A Robust System

In the remainder of this paper, such a system is referred to as a "robust" system (see Figure 4). We define a robust system as one which, when implemented and operated without error, maintains data in an unencrypted form to the least extent commensurate with the fundamental operations of computing.

The cloud is essentially an instantiation of Figure 4 but also spans jurisdictions and continents.

VI. Responses to Threats

This section begins by examining existing responses to the individual threats and then argues that such responses may be ineffective against the combined threat of the "robust" system.

A. Response to the encryption threat

An obvious approach to the encryption-based threats would seem to be to attack the encryption that protects "robust systems". Over time, resources and a concentrated research effort the technologies that make up the "robust system" might well be broken and a way found to reveal the data needed for forensic reconstruction. This would, however, be a something of an "own-goal" for the computer security community that has been making computers progressively harder to break into. The same technologies that protect the terrorist's plot also guard individual privacy, the world's e-commerce systems and bank accounts. We, as a society, ought to have no interest in breaking this encryption other than to identify weaknesses in protecting our own data.

B. Response to Full Disk Encryption (FDE)

Rather than use a technical approach to get around the protection offered by FDE, the UK response (as embodied in Regulation of Investigatory Powers Act (RIPA) Part III, Section 49 [32]) has been one based on legislation. Failure to disclose a password/decryption key following the service of an appropriate court order is now an offence carrying a maximum penalty of a two year custodial sentence (or 5 years in the case of a threat to national security). In the year 2014/2015, 37 "Section 49" notices were issued. 22 refused to comply and three were convicted [33].

It is interesting to note that the initial response to FDE, when it emerged as a threat, was not to try to produce a faster decryption technique, but rather a move towards live-forensics in which a logical image of a machine is taken via a login session during which the necessary decryption keys have already been provided. This move may not merely be because of the undoubted practical difficulty in producing such a technique, but rather that the research cryptographers and cryptanalysts are on the same side. This observation leads to the notion that the threats outlined above should not be considered purely as a computer science problem, but rather as one to which operational solutions might also be applied.

C. Response to Anonymous Routing

When, during World War 2, the cryptanalysts of Bletchley Park were faced with a "blackout" of decrypted signals traffic due to a change in enemy ciphers, some level of useful intelligence was derived from the practice of "traffic analysis". Crudely stated, this allowed the origin and destination of a message to be identified even if the content of the message could not be deciphered. By correlating the volume of traffic between known signal stations, areas of significant enemy activity could be identified. Unfortunately, faced with a similar blackout on intercepting internet traffic due to securely encrypted communications, modern digital forensic investigators may be denied even this limited option.

 ISBN: 978-1-61208-607-1

1) TOR Weaknesses: The current implementation of TOR is vulnerable to certain attacks, which could offer a means of traffic analysis as evidence [34], [35]. However, work is on-going to remove those vulnerabilities [36]

D. Response to Robust Security.

Currently, responses to the combined threat would be difficult, primarily because of the way that the cloud makes the problem trans-jurisdictional. This presents the twin problems of practical international cooperation and the differing legal attitudes to encryption.

E. Response to Cloud

The most appropriate responses to the threats posed by cloud computing lie outwith the purely technical domain and are more concerned with obtaining the cooperation of the cloud providers and jurisdictions where the servers are located.

VII. SOLUTIONS

This section outlines some possible options for maintaining access to evidence in the face of individual threats combining to offer "robust" security. This paper does not seek to suggest that such solutions are either desirable or practical, merely that they are technical possibilities.

A. Acquire evidence that is in the clear

The concept of an "attack surface" is familiar in the computer security world. It seems reasonable in the role-reversed world of the digital investigator trying legitimately to gain access to a suspect system. Whilst the "attack surface" of the "robust system" is minimal it is not non-existent. In the short-term, one technical response to the encryption-based threats is increased reliance on live forensics. Depending as it does on gaining access to a suspect system whilst it is turned on, and while the user logged in with decryption keys having been supplied, it is an option with its practical difficulties. The challenge here is to provide law enforcement with the legislative framework and operational capability routinely to use such techniques on a large scale.

Other technical means of exploiting the reduced attack surface include covert surveillance of screen and printer output by video or the Van Eck technique [37], for example. Difficulties here are obtaining permission to mount the surveillance and the logistics of putting suitable equipment in place, undetected.

The "robust system" concept includes the idea of perfect implementation and, of course, practical systems rarely are. The greatest source of potential weakness of any cryptosystem can be human error, and it is thus reasonable to conjecture that exploiting security implementation or human errors may continue to provide an evidence source long into the future.

B. Black-bag techniques

The hacker community has (and continues to have) great success in gaining illegal access to insufficiently-secured systems, both by technical means and by social engineering. The adoption of some of their techniques (e.g., "black-bag" cryptanalysis [38]) to provide evidence would be challenging from the current rigid legal point of view on admissibility of evidence and the issue of "forensic soundness" [39]. It may be that this stance needs to be modified in order to allow evidence recovered using non-standard means.

Two examples of techniques that have emerged from this community that might be useful are:

- The use of **key-loggers** (both software and hardware) is a well-known hacking technique. However, employing it for evidence gathering counts as the interception of communication and thus requires appropriate authorisation.
- The **Firewire direct memory access (DMA) hack** [40] allows direct access to a system's memory via a firewire port. It offered a means of rapidly imaging a target system's RAM (and potentially the disk) without the need to install and execute software on the target (or indeed alter the state of the RAM).

C. Forensic Readiness/Analysable by design

One possible mitigation might be to universally adopt the discipline of "forensic readiness" [41], in which all systems record their activities and make such a (cryptographically protected) record accessible to law enforcement in a retrospective manner, as required. Three questions emerge: **(a)** is it technically possible? **(b)** is it practical? and **(c)** is it desirable?

1) Technical Feasibility: The question of possibility can be broken down into recording and access aspects.

- **Recording** Part of the discipline of forensic readiness deals with the configuring of operating systems and applications to record their operation in sufficient detail to enable meaningful reconstruction of their usage [42]. Such techniques are commonly deployed on organisational systems rather than those of the private home user. Various suggestions as to how to make operating systems leave analysable artefacts as part of their natural operation have also been put forward, including [43]. These arguments coupled with the ever-increasing capacity of storage device (and consequent decrease in storage costs) make it reasonable to suggest that such forensic logging is feasible.
- **Access** For reasons of security, such a log should be encrypted. Providing a way into it, thus becomes a matter of accessing the appropriate key.

Current practice in dealing with encryption keys falls under two headings: *key escrow* and *key surrender*. The difficulties associated with key escrow (primarily assuring the security of held keys and designing access mechanisms) have prevented its widespread adoption. Although there are civil liberties problems associated with both forms of key access, the UK has adopted a "key surrender" policy. With a lack of outcry (and possible due scrutiny) that surprised commentators, a policy of Government Access to Keys (GAK) was embodied in the Regulation of Investigatory Powers Act (RIPA) 2000. Failure to disclose an encryption key when presented with a court order demanding its release to an appropriately authorised government agency carries a maximum custodial sentence of 2 years (five years for terrorism and child pornography offences). An as yet unimplemented provision of RIPA allows for a sentence associated with the crime under

 ISBN: 978-1-61208-607-1

investigation to be imposed should keys be withheld (i.e., if a suspect is being investigated for murder, and refuses to divulge a key, then the full sentence for murder could be applied). Whilst the length of sentence can be debated, this mechanism at least provides a means of dealing with an unwillingness to divulge keys.
It seems reasonable to assume that any keys protecting a forensic log could be dealt with in a similar manner.

2) Practicality: The techniques of forensic readiness are in the domain of the workplace. IT departments could activate forensic readiness, but there is little incentive for private users to do so and obviously there is a considerable disincentive for anyone planning to commit a cybercrime.

For an evidence database to exist universally, it would have to be built into the system (presumably by system manufacturers at system-build time) and turned on (possibly without the option to turn it off) by default.

For the (non-technical) majority of users, this might suffice to provide a means of acquiring evidence should the need arise. Achieving the necessary universality is more problematic as suitably knowledgeable users could simply construct their own non-forensic-ready system using existing technology. Thus forensic-ready devices will only be adopted by the law-abiding, in whom we have no interest.

A similar legislative technique to that used with encryption technology could be employed, i.e., make it an offence to operate a computer that is not forensically ready. This strategy would suffer from the same "presumption of guilt" objection that accompanies a sentence under RIPA, as well as the difficulties of coping with legacy systems. It is also unclear how well such a strategy might scale as computing becomes ever closer to realising Weiser's vision of the ubiquitous computer [44].

A technical alternative to legislation might be to put in place a requirement for forensic-readiness before a device can access the Internet. Aside from the technical difficulties with enforcing this, and problems with universal adoption in different jurisdictions, how long would it be before an alternative "Dark Internet" arose?

A further practical difficulty is associated with resourcing such a scheme. Encryption is not yet widespread and many police forces report a considerable backlog of digital forensics cases. It is by no means clear that current administration systems could cope with the added burden of obtaining court orders for evidence-log disclosure.

3) Desirability: As a society, we have accepted the desirability of law-enforcement being able to access private, encrypted data, in appropriate circumstances, via RIPA 2000 and legislation of similar purpose in other jurisdictions. It might thus seem that enforcing the deliberate availability of something from which forensic reconstruction of user activity might take place would be equally acceptable. After all, no eyebrows are raised at the current ability to reconstruct the same information as part of an investigation from the traces 'accidentally' left behind by the Operating System. However, evidence-gathering techniques that require the active capture of information are seen as an interception of communications and require higher permission. A distinction is thus made between the *a-priori* capture and the post-hoc reconstruction of (potentially) identical information. The techniques of forensic readiness fall across this divide by capturing data but not allowing its authorised examination until after an event.

The distinction between *a-priori* and *post-hoc* evidence is based on the need to preserve privacy: If a crime has been committed then it is proportionate to acquire and reconstruct evidence, however if a crime is only anticipated, then higher permission for state intrusion upon the privacy of an individual is required.

How should the use of forensic-readiness based evidence thus be regulated? The proposal here is that it becomes a routine technique and, for reasons of cost, speed and efficiency there should be a low barrier to its use.

Stallman [45] has argued against the idea of the "treacherous computer", which the current forensic readiness proposal might be thought to embody. However, a scheme in which the keys that protect the forensic readiness backdoor belong to the owner of the equipment, and are only used in the case of an investigation, may offer sufficient protection from this charge.

The proposed forensic readiness scheme is predicated on the (negative) incentive of a custodial sentence to gain access to the necessary keys. Such a practice can give rise to concerns over its abuse.

Another potential problem is the security of the back-door itself. If it were universally deployed, then one break in would compromise everyone's security. The counter argument here is that such a scheme is only necessary to counter "robust security" in the first place.

4) Cloud Forensics Readiness: If cloud systems could be made forensically ready, then obtaining evidence is at least technically possible. Ensuring that the necessary legislation is in-place and enforceable globally is another matter. The primary objection to this is the *trans-jurisdictional* nature of the Internet. Whilst the creation of a separate jurisdiction for the Internet has been proposed [46], such solutions are a long way from realisation. Obtaining appropriate international cooperation is, however, a human problem rather than an insoluble cryptographic one. Human problems, while seeming intractable, can often be solved in ingenious ways, so this offers some hope.

5) Forensics Readiness Conclusion: The forensic readiness scheme outlined above is, at best, a compromise. Enforcing its universal deployment seems problematic and it maybe that in a "robust security" scenario we might simply have to accept that it offers no hope against the determined, cybercriminal with the knowledge to set up their own system. However by building it into new devices, forensic readiness may offer some utility against the average user who does not fiddle with the security settings.

D. Fundamental Changes

Two extremely fundamental changes would also serve to make things easier in terms of digital forensics. The first is that the Internet no longer permits or supports anonymity. If every Internet user has to prove their identify in an irrefutable way to be permitted to use the Internet, it would make attribution much easier to prove. This does, of course, compromise individual privacy, and might not be an acceptable solution.

Another suggestion is that the Internet be treated as a separate jurisdiction, much as is the case for independent

 ISBN: 978-1-61208-607-1

countries. We would then be able to have laws that apply across the Internet. This removes the need for forensics investigators to negotiate multiple jurisdictions in order to carry out an investigation. This would have to be accepted by nearly 200 independent countries across the planet, so is probably infeasible.

VIII. CONCLUSIONS

Advances in computer security may be about to nullify many of the current digital forensic techniques. Even if the blackout is not total, now is the time to start thinking about what happens, and what our options could be. One possible option is the widespread use of a cryptographically protected forensic readiness approaches with the disclosure of the keys subject to laws similar to the UK's RIPA.

Despite civil liberties concerns, we have, as a society, already taken the step of demanding access to encryption keys when necessary. Should we take the additional step of demanding some form of universal forensic readiness?

Ultimately, this is not a technological debate about how to facilitate a digital forensic investigation; rather it is an ethical question about whether an individual has the right to keep secrets from the state. In the encryption debate, we have already decided that the answer is "no." Currently a compromise exists whereby those with appropriate technical skills and knowledge can achieve a much greater degree of privacy than the average citizen. The proposed approach might remove such inequality.

Before developing such a technology, exceptionally careful consideration should be given to the ethical implications of the use of the technology — assuming the moral neutrality of the technology and the acknowledgement that the investigators may not always be the "good guys". Of course, there is a debate in the computer ethics literature as to whether technology is value neutral or not, for example, see Johnson [47]

The evidence blackout is not yet with us, but appropriate forensic readiness measures and legislation would take time to develop. In the short term, it is possible that a greater emphasis on surveillance and live seizure will be necessary, along with an appropriate legal and operational framework.

The real challenge to the security/digital forensics community is that we, as the ones who understand the technical issues and their consequences, must be the ones who lead the debate.

REFERENCES

[1] J. C. R. Licklider, "Memorandum for members and affiliates of the intergalactic computer network," 1963, originally distributed as a memorandum April 23, 1963. Published on KurzweilAI.net.

[2] N. N. Rojas, "CRM Review," undated, http://erpsoftware360.com/salesforce.htm Accessed 6 December 2017.

[3] D. Catteddu, "Cloud Computing: benefits, risks and recommendations for information security," in Web application security. Springer, 2010, pp. 17–17.

[4] R. McKemmish, What is forensic computing? Australian Institute of Criminology Canberra, 1999.

[5] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, vol. 9, no. 2, 2012, pp. 71–80.

[6] A. Kerckhoffs, "Military cryptography," Journal des sciences militaires, 1883, p. 5–83.

[7] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, 2010, pp. S64–S73.

[8] J. Rubin, J. Queally, and P. Dave, "FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now," 2016, march 28 http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html Accessed 6 December 2017.

[9] J. J. Roberts, "The FBI Can't Open the Phone of the Texas Church Shooter Devin Kelley, note=http://fortune.com/2017/11/08/texas-church-shooting-fbi-phone/, accessed november 8 2017,," 2017.

[10] G. Burton, "Amber Rudd: The little people don't need encryption," 1 August 2017, the Enquirer https://www.theinquirer.net/inquirer/news/3014855/amber-rudd-the-little-people-dont-need-encryption Accessed 6 December 2017.

[11] Masnick, "Theresa May Tries To Push Forward With Plans To Kill Encryption, While Her Party Plots Via Encrypted WhatsApp," 12 June 2017, https://www.techdirt.com/articles/20170611/11545237565/theresa-may-tries-to-push-forward-with-plans-to-kill-encryption-while-her-party-plots-via-encrypted-whatsapp.shtml Accessed 6 December 2017.

[12] N. Statt, "Donald Trump thinks he can call Bill Gates to 'close up' the internet," 7 December 2015, https://www.theverge.com/2015/12/7/9869308/donald-trump-close-up-the-internet-bill-gates Accessed 6 December 2017.

[13] R. Roberts, "Prime Minister claims laws of mathematics 'do not apply' in Australia," 15 July 2017, http://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html Accessed 6 December 2017.

[14] D. Hilley, "Cloud computing: A taxonomy of platform and infrastructure-level offerings," Georgia Institute of Technology, Tech. Rep., 2009.

[15] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in IFIP International Conference on Digital Forensics. Springer, 2011, pp. 35–46.

[16] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, 1979, pp. 612–613.

[17] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," Journal of the ACM (JACM), vol. 36, no. 2, 1989, pp. 335–348.

[18] J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, and P. *et al.*. Eaton, "Oceanstore: An architecture for global-scale persistent storage," ACM Sigplan Notices, vol. 35, no. 11, 2000, pp. 190–201.

[19] J. J. Wylie, M. W. Bigrigg, J. D. Strunk, G. R. Ganger, and H. *et al.*. Kiliccote, "Survivable information storage systems," Computer, vol. 33, no. 8, 2000, pp. 61–68.

[20] A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed systems, vol. 14, no. 9, 2003, pp. 885–896.

[21] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on, 2008, pp. 5–13.

[22] E. Casey and G. J. Stellatos, "The impact of full disk encryption on digital forensics," ACM SIGOPS Operating Systems Review, vol. 42, no. 3, 2008, pp. 93–98.

[23] "VeraCrypt," https://veracrypt.codeplex.com/ Accessed 6 December 2017.

[24] "BitLocker," https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-overviewAccessed 6 December 2017.

[25] G. E. Suh, C. W. O'Donnell, and S. Devadas, "Aegis: A single-chip secure processor," IEEE Design & Test of Computers, vol. 24, no. 6, 2007, pp. 63–73.

[26] R. B. Lee, P. Kwan, J. P. McGregor, J. Dwoskin, and Z. Wang, "Architecture for protecting critical secrets in microprocessors," in ACM SIGARCH Computer Architecture News, vol. 33, no. 2. IEEE Computer Society, 2005, pp. 2–13.

[27] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," Foundations of secure computation, vol. 4, no. 11, 1978, pp. 169–180.

[28] C. Gentry, "Fully homomorphic encryption using ideal lattices." in STOC, vol. 9, no. 2009, 2009, pp. 169–178.

 ISBN: 978-1-61208-607-1

[29] J.-S. Coron, D. Naccache, and M. Tibouchi, "Public key compression and modulus switching for fully homomorphic encryption over the integers." in EUROCRYPT, vol. 7237. Springer, 2012, pp. 446–464.

[30] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," IEEE Journal on Selected areas in Communications, vol. 16, no. 4, 1998, pp. 482–494.

[31] J. Siegfried, C. Siedsma, B.-J. Countryman, and C. D. Hosmer, "Examining the encryption threat," International Journal of Digital Evidence, vol. 2, no. 3, 2004, [PDF].

[32] UK Government, "Regulation of Investigatory Powers Act 2000," http://www.legislation.gov.uk/ukpga/2000/23 (downloaded 2013).

[33] Open Rights Group, "Regulation of Investigatory Powers Act 2000/Part III," https://wiki.openrightsgroup.org/wiki/Regulation_of_Investigatory_Powers_Act_2000/Part_III#Cases Accessed 6 December 2017.

[34] M. Kumar, "Tor anonymizing network compromised by french researchers," 2011, http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html October 24 (downloaded April 2013).

[35] R. Lemos, "Tor hack proposed to catch criminals," http://www.securityfocus.com/news/11447 SecurityFocus 2007-03-08 (downloaded April 2013).

[36] "TOR," Online,https://www.torproject.org/ (downloaded April 2013).

[37] W. Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" Computers & Security, vol. 4, no. 4, 1985, pp. 269–286.

[38] R. Divya and S. Muthukumarasamy, "An impervious qr-based visual authentication protocols to prevent black-bag cryptanalysis," in Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. IEEE, 2015, pp. 1–6.

[39] E. Kenneally, "Confluence of digital evidence and the law: On the forensic soundness of live-remote digital evidence collection." 2005, sSRN Papers https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145647 Accessed 6 December 2017.

[40] "Technical notes, my online memory," undated, http://ilostmynotes.blogspot.co.uk/2012/01/firewire-and-dma-attacks-on-os-x.html Accessed 7 December 2017.

[41] R. Rowlingson, "A ten step process for forensic readiness," International Journal of Digital Evidence, vol. 2, no. 3, 2004, pp. 1–28.

[42] A. Poulter, I. Ferguson, D. McMenemy, and R. Glassey, "Question: Where would you go to escape detection if you wanted to do something illegal on the Internet? Hint: Shush!" Global Security, Safety, and Sustainability, 2009, pp. 1–8.

[43] F. Buchholz and E. Spafford, "On the role of file system metadata in digital forensics," Digital Investigation, vol. 1, no. 4, 2004, pp. 298–309.

[44] M. Weiser, "The computer for the 21st century." Mobile Computing and Communications Review, vol. 3, no. 3, 1999, pp. 3–11.

[45] R. Stallman, Free software, free society: Selected essays of Richard M. Stallman. Lulu.com, 2002.

[46] J. M. Oberding and T. Norderhaug, "A separate jurisdiction for cyberspace," Journal of Computer-Mediated Communication, vol. 2, no. 1, 1996, pp. 0–0.

[47] D. G. Johnson, "Is the global information infrastructure a democratic technology?" ACM SIGCAS Computers and Society, vol. 27, no. 3, 1997, pp. 20–26.

 ISBN: 978-1-61208-607-1