doi:10.1017/aju.2017.3

SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

A COMPUTER SCIENTIST MUSING ABOUT THE DNC HACK

*Fred B. Schneider**

Introduction

Theft of secrets is nothing new. Nor is it new to publicize stolen secrets with hopes of influencing (or instigating) leadership changes in government. So the theft of confidential information being stored by the Democratic National Committee (DNC) is part of a long tradition, albeit perpetrated in a new venue: cyberspace. This new venue, however, offers considerable benefits to attackers:

- **Remote Access**. An attacker can work any time of day or night, which not only helps evade detection but also allows attacks to proceed over an extended period. Moreover, a skilled attacker is able to remove evidence of the attack. Electronically exfiltrating secrets, for example, does not require removing or altering anything physical and thus does not have a noticeable effect. In addition, even if a cyberattack is detected, attribution is difficult. Consequently, deterrence through accountability is not an effective defense. Even when attribution is possible, knowledge of who perpetrated some attack is actionable only if some law enforcement regime has jurisdiction over the attacker. By working from abroad, an attacker often can use jurisdiction to evade punishment.
- **Speed**. A large part of the cost for perpetrating an attack in cyberspace is the effort to penetrate the target computing system. Once that system has been compromised, existing high-speed networking enables large amounts of information to be rapidly transmitted back to the attacker. Thus, an attacker's exposure is small, even to exfiltrate large numbers of documents. And the additional effort and exposure to steal further information from the target is inconsequential. So attackers are not forced to decide before or during an attack which individual documents to steal—it's just as easy to steal everything and digest it later, on the attacker's own system.

The DNC attacks were successful for two reasons.

1) Passwords are not a secure way to authenticate whether somebody should be granted access to a system. They are easily guessed or stolen.

2) Commercially available computing systems are rife with vulnerabilities. They, in turn, can allow a program running under the auspices of one user to access data that should be accessible only to other users.

* *Samuel B. Eckert Professor of Computer Science and Chair, Department of Computer Science at Cornell University*

Yet we do know how to do better. Such systems, however, are less convenient to use and more expensive to develop. Better authentication requires that users engage in more complicated protocols, and do so more often. Elimination of system vulnerabilities requires developers to expend more effort in design and testing. System developers also would have to eschew the complicated features users favor and, instead, build only those features that are simple enough for all behaviors to be anticipated and analyzed. And tighter access polices would have to be formulated individually for each object.

Higher cost? Less convenience? These sacrifices require some value proposition. But today it is hard to justify making those sacrifices for security:

- The need for better security is not well understood by those who make procurement decisions. Institutions are hesitant to broadcast that they have been attacked successfully, since that knowledge detracts from their image. Moreover, information about threats is typically held close by those who know. So decisions to make sacrifices must be made without an accurate picture of the risks that come from failing to make those sacrifices.
- Good metrics for system security do not exist, and there are technical reasons to believe they cannot exist. Sacrifices for security must then be rationalized by appeal to indirect measures, such as the reputation of the software producer or the development process that was employed. By their nature, indirect measures cannot give a strong guarantee of security.

So system producers, purchasers, and users have no way to justify the costs—be it inconvenience or other forms of expense—for system security. Furthermore, existing law provides the wrong incentives to software producers, if system security is what we seek: producers are not legally accountable to their customers or to anyone else when a system they sell has flaws that make that system vulnerable to attack. We might change the law. To do so, however, means selecting some mix of taxpayers, users, or investors to bear the burden of higher costs and/or reduced functionality.

Help from Cryptography?

Without knowledge of the decryption key, nothing can be learned about the contents of an encrypted document. So cryptography transforms the implementation of confidentiality for a set of documents into the much simpler problem of controlling confidentiality and access to a decryption key. Today's commercial computing systems are capable of storing documents on disk in encrypted form, though this feature is rarely used. When encryption is not in use, an attacker masquerading as some user *U* would likely have free reign not only to access any document that *U* can view but also any document that any other user was authorized to view. Encrypt all the documents and such an attacker would only be able to view the documents that *U* is authorized to view plus, in the worst case by exploiting vulnerabilities, the few documents being accessed by other users while the attack is in progress.

Interception of messages in transit on a network affords attackers a second means for stealing secrets. But if message contents are encrypted, then interception reveals less. However, even this form of surveillance can reveal useful information, because the destination of a message will not be encrypted—a destination address must remain intelligible, so it can be read by network switches that implement message routing. Knowledge of a message destination might reveal the identity of groups that wished their involvement to be secret. On balance, however, encryption for data in motion has an enormous pay-off for protecting the confidentiality of information.

Given the improved security that results from encryption for data at rest and for data in motion, we might hope that press attention from attacks would prompt wary users to insist on email and file system encryption, visionary system administrators to be proactive and activate those features on systems they manage, and/or well-meaning

https://doi.org/10.1017/aju.2017.3 Published online by Cambridge University Press

software developers to make encryption the default for systems they distribute. Hope springs eternal. The DNC computing system compromise was not the first highly-publicized confidentiality breach. It was not even the first confidentiality breach to have national security implications. For example, the attack of the U.S. Government Office of Personal Management (OPM) around March 2014 stole identify data for all who hold security clearances.

Regulation is a means to promote action for greater societal benefit when neither common sense nor the market provide the incentives. So it is tempting to contemplate laws that would incentivize encryption—at least for certain kinds of information. There is, of course, the problem of characterizing what information should be covered by such a law. But encryption also raises a far more contentious issue, which puts two societal goals in conflict: surveillance versus security.

Surveillance provides a cost-effective approach to defense for any collection of assets in an asymmetric setting. It enables the defender to anticipate a given attack. Forewarned, the defender can then undertake modest preemptive action and/or deploy limited defenses that temporarily protect the threatened asset from the expected attack. The total cost of this surveillance-based approach to defense is significantly lower than the total cost to deploy individual defenses for every asset that might be attacked—the cost of a surveillance-based defense is the cost of surveillance (which is proportional to the number of attackers or to the number of sensors that provide sufficient coverage) plus the cost of defenses that can be proactively deployed in response to an alarm.

The rationale for surveillance-based defense is not only compelling, but there is ample evidence that the approach is widely used in practice. The Snowden disclosures revealed that, in order to anticipate terrorist attacks, the U.S. Intelligence Community has been intercepting Internet messages in transit to international destinations. And cell phones are increasingly seen by law enforcement as a source of valuable information, not only about an individual's past activities—useful for forensics—but also about planned activities and collaborators.

Encryption, however, impedes surveillance and impedes access to information stored on devices procured using search warrants. So encryption undermines what has become an important approach to U.S. defense, hence to U.S. security. Calls for wide-spread deployment of encryption have been characterized as "Going Dark" when discussing any transition to a regime where file systems and network traffic is encrypted. So we see legislative proposals (e.g., Burr-Feinstein[1]) advocating that encryption mandates be accompanied by a mandate to provide some form of "back door" for decrypting the encrypted information, and we see Federal officials (e.g., FBI director James Comey[2]) advocating that access to such a "back door" be controlled by some body that can be trusted to make sensible trade-offs between the rights of individuals and the security of our nation.

To some, putting trust in a surveillance-authorizing body is problematic. Moreover, transparency for review of that body's decisions might not be an option here, since surveillance often becomes ineffective when the target has been warned. So we could be forced to delegate decisions about surveillance to a body without the benefit of deterrence through accountability that oversight provides. Information encrypted by the DNC would be an interesting *gedankenexperiment*, given the strong incentive for a political party in power to preserve the status quo. Encryption here might have protected DNC secrets from a foreign adversary but not from the domestic one.

Of course, there already are various government bodies that U.S. citizens trust to operate in secret, making decisions where the rights of individuals are in tension with greater societal good. The above "back door" argument raises another class of concerns, too, though. Is it technologically feasible to ensure that a surveillance-authorizing body is the sole principal with access through some "back door"? A long history of failures suggests that skepticism is justified. So we are unlikely to succeed in discharging one of the fundamental requirements for "back

[1] Discussion draft, A Bill to require the provision of data in an intelligible format to a government pursuant to a court order, and for other purposes, 114th Cong. (2015).

[2] Sally Quillian Yates & James B. Comey, Statement before the Committee on the Judiciary United States Senate at a hearing entitled "Going Dark: Encryption, Technology, and the balance between Public Safety and Privacy" (July 8, 2015).

https://doi.org/10.1017/aju.2017.3 Published online by Cambridge University Press

door" access to encrypted content. Regulation that mandates encryption becomes less compelling to encryption advocates if that regulation also must mandate a "back door."

The Bigger Picture

Absolute security is widely understood to be a fool's errand; system security is best seen as relative. We deem a system to be secure provided it enforces some specified policies, even while being attacked by some class of adversaries. Examples of policies might include:

1) confidential information is not disclosed to unauthorized users,

2) information is not changed by unauthorized users.

3) requests for service are handled within T seconds.

Classes of adversaries often are characterized in terms of their resources or technical capabilities. We therefore should be regarding nation-state intelligence agencies, domestic activist groups, local organized crime, and college undergraduates as being distinct classes, since each would have access to different levels of resources. The theft of secrets from the DNC computing system violated policy (1) above, as did the OPM breach. In both of these cases, it would seem reasonable to have anticipated a nation-state adversary. Sony, whose compromise in Fall 2014 revealed sensitive enterprise information, might justifiably have been preparing to defend only against weaker adversaries. But those defenses might not have sufficed if, as reported in the press, North Korea was behind the attacks.[3] Deciding on an appropriate defense is difficult when deciding on potential adversaries is difficult.

In addition, as the discussion of cryptography reveals, enhanced security of computing systems can be in tension with other values that governments deem important. So there are some aspects of improved cybersecurity that a government is unlikely to promote. Here is a case where the government might not be willing to create incentives when each individual's behaviors fails the greater societal good.

Finally, as should be clear, the DNC attacks, while a good reason to start a discussion, could easily lead us astray. That campaign secrets could destabilize a presidential election is beside the point (and is something that the U.S. has reputed to have done to others, too[4]). In seeking an approach to remedies, we should focus on remedies that apply to a broad range of institutions. As long as our systems are used by ordinary people, then we should authenticate users in ways that are difficult for an attacker to circumvent by fooling the victim into abusing authority. And as long as our systems are used to store information, then cryptography should be deployed to help protect data at rest as well as data in motion.

[3] The assault on private institutions by nation-state adversaries complicates analysis used to justify investments in defenses. It also creates externalities that justify a role for government in previously unregulated sectors. Moreover, incentivizing the victims of these cyberattacks to enhance their defenses is not the point of greatest leverage. Efforts by the software producers are higher leverage, because systems they sell are, by and large, not sector specific and are widely used.

[4] Ishaan Tharoor, *The long history of the U.S. interfering with elections elsewhere*, WASH. POST (Oct. 13, 2016).

https://doi.org/10.1017/aju.2017.3 Published online by Cambridge University Press