ENCRYPTION FOR JOURNALISTS – BY ENG. MARTIN OBUYA, AMB. GOVT. AFFAIRS, IHUB

Background

Journalists, not usually known for their computing skills, may be unsure how to go about familiarizing themselves with the various techniques for encrypting their communications and data. This section, therefore, hopes to introduce a number of tools and concepts, together with resources for continued learning; hopefully, it can provide the basis for journalists to begin the journey.

All the tools detailed below, unless stated otherwise, are open-source and freely available for Windows, Mac OS X and Linux operating systems. Given the high chance that Windows and Mac OS X are compromised, it is recommended to use Linux in situations where security is critical.

Naturally, as with all software, bugs and security problems are constantly being found (and hopefully fixed); it goes without saying that the latest (stable) version of all the following tools should always be used, and security warnings on the developers' websites checked regularly.

For critical applications, one should already be familiar with the tools in question to avoid potential errors that could compromise security. Most of the tools described below provide comprehensive guides that should be studied carefully.

Passwords

Many of the encryption methods detailed below involve the use of a password. The importance of using good passwords cannot be overstated. This is true also for passwords linked to email and other online accounts, though one should take particular care in picking good passwords for encryption as this will determine its reliability.

For example, using a strong encryption method but with 'abc' as password is hardly better than using no encryption at all, at least in situations beyond the most trivial. A good password is one that is relatively long (more than 10 characters), involving upper- and lower-case characters, numbers, special characters such as # and *, and not using any words that can be obviously linked to you.

Communicating securely

Most widespread tool for encryption of emails is PGP (**Pretty Good Privacy**), and its open source implementation GPG (**GNU Privacy Guard**). These tools use the encryption algorithm known as RSA, named after its creators Rivest, Shamir and Adelman.

This method relies on two keys: one, the public key, is usually shared online (for example, via a personal homepage or through key servers and enables third parties to encrypt messages they wish to send; and the private key, without which the encrypted message cannot be decrypted and read.

Note that the sender of the encrypted message need not have ever met the recipient; however, they must at least trust that the public key (and associated email address) genuinely belongs to them.

It is important to understand that the strength of RSA relies on a mathematical belief: that very large integers (with hundreds of digits) are difficult to factor (that is, reduce to its prime components).

While no known method exists to do this in any reasonable space of time, this does not preclude the possibility that one will be found in the future.

One important factor in the security of RSA is the key size used (measured in bits), which are generally powers of 2 greater than 1024. To be safe, a key size of 4096 bits or more is advised. Another consideration is the implementation of RSA being used.

CFI 4M INTERNATIONAL MEETING, 20-21 APRIL 2016, PARIS, FRANCE

A Swiss study found that an alarming number of public keys available on the internet shared common factors; the likely reason being sloppy implementations and small key sizes. Given their wide use and history, PGP and GPG can be assumed to be among the most reliable implementations at present.

Another capability of RSA besides encryption is that of digitally signing emails and data (this involves using your private key to encrypt – then your public key can be used by anyone to decrypt it and check that the result is the same as the message in question).

Such a signature can be used by the recipient of data to confirm that the email has not been tampered with in transit. This is particularly important if an email account is hacked, as it can be used to prove that an account has been compromised.

Instant messenger
For real-time communications, an account on the real-time messaging network **Jabber**, together with an open- source chat client such as **Pidgin**, allows encryption of messages using the **OTR** ('off the record') plugin. Documents indicate that the NSA is unable to decrypt OTR-encrypted chats.

With both methods described above, communications are only safe once keys have been exchanged and verified via a different communication channel (voice- based is preferable as it is difficult to imitate), where the identity of the intended recipient can be confirmed.

This is to avoid so-called man-in-the-middle attacks, which may best be explained with an example. Say that Amina and Bakari wish to communicate securely, and are presently in physically different locations.

If Amina emails Bakari requesting his public key (in order to send him an encrypted email), Amina has no way of knowing if Bakari's email account has been hacked (by Ida, say) and an alternate public key (for which Issa owns the private key) sent in the reply instead.

If Amina simply uses this key to send an encrypted email with sensitive information, Ida will be able to decrypt it. Hence the importance of verifying keys through another channel – in this case, Amina can simply call Bakari and verify the key he emailed is, indeed, his own key.

Note that this channel need not be encrypted – in fact, even if Ida is listening in, unless she can change Bakari's voice in real-time in a way that convinces Amina, there is no problem (so long as this channel is only used to verify keys). In practice, it is not the key that is verified but its fingerprint, a much shorter string of characters that is used to identify the key itself.

Encrypting files
In addition to encrypting communications, journalists will often need to encrypt documents they are working on, such as articles in progress or documents passed to them in confidence. Commonly used compression tools often provide encryption support; though commercial tools are potentially compromised and should not be trusted.

A reliable open source compression tool is **7zip**, which supports the AES-256 encryption standard. The strength of the encryption will be compromised by a trivial password.

Another popular tool is **Truecrypt** (not strictly open-source, though the source code is available), which offers a wider range of cryptographic functions, such as encrypting entire file systems.

It is worth noting that extra care may be needed when working with particularly sensitive information. Any computer connected to the internet is potentially at risk of being spied on. In such a situation, the sensitive data can be accessed before it is even encrypted.

An extra level of care that can be taken is to buy a new computer, which is never connected to the internet, and used solely for the purpose of working on, encrypting and decrypting sensitive files (this is known as 'air-gapping'). This way, the plaintext (non-encrypted) data will never be loaded into memory on an online computer.

Accessing the internet anonymously

When connected to the internet, our identity is revealed by a unique IP (internet protocol) address. Each connection we make on the internet (to websites, email servers and so on) may be traced back to us with this address.

What this means is that even with prudent use of encryption, the identity of whistleblowers and those they work with can be uncovered (though what they are saying may not be). Because of this, and depending on the situation, anonymous access to the internet may be desired.

One of the simplest ways of achieving this is with the **Tor** software package, which anonymizes connections by sending them through a series of intermediate nodes (computers running the Tor software in 'relay' mode), before finally accessing the website through the final node in the chain, the exit node.

One important point to note is that while communications within the Tor network are encrypted, the exit node will transmit data as it was at the beginning – in other words, the user is responsible for encrypting their communications. Failure to do so can compromise anonymity.

Care should also be taken when links are followed, since external applications (for example, when opening a linked PDF file) opened will not be running through Tor by default and can unmask you.

While there are a number of potential issues with Tor, and new vulnerabilities are often being found, it is still believed to be a reliable way to achieve anonymity online. Indeed, the NSA's own exploits of Tor have focused on the Firefox web browser supplied with the Tor Browser Bundle (these exploits have since been fixed), not the Tor system itself.

Despite this, the Tor Browser Bundle is still recommended (the website states: 'almost any other web browser configuration is likely to be unsafe to use with Tor') – just make sure to always use the latest version.

Another way of anonymizing oneself online is to purchase an account on a VPN (Virtual Private Network) service. In a nutshell, this simply serves as a relay point for your connections; the IP address you appear to be connecting from is that of the VPN server, not your personal computer.

Data is encrypted between your computer and the VPN servers (though it should be noted that this is one of the types of encryption that the NSA has worked to compromise).

There are a large range of VPN services available, with varying levels of security. One word of caution: many VPN services will log all user activity and hand over this information when pressured by governments and law enforcement.

For true anonymity, a VPN provider that does not log user activity is essential; AirVPN and PrivatVPN are two providers that claim not to.

Note that Tor and VPNs can also be used to access websites that have been blocked. In countries which operate particularly aggressive censorship of the internet, such access to sites routinely used by journalists such as Twitter may be restricted; a VPN account allows you to bypass such filters regardless of physical location.

The all-in-one solution: TAILS

Tails is a customized version of Debian Linux which has most of the tools discussed above pre-loaded and uses Tor by default to connect to the internet. Importantly, it can be installed on a USB key and used to boot directly into the operating system.

Once sensitive tasks have been completed, you can boot back into your usual operating system and no trace of the Tails session will remain.

This is the easiest way to get up and running with encryption and anonymity with the least chance of a mistake, but note also that it is not suitable to use as a day-to-day operating system and should only be used to carry out sensitive tasks.

Blowing the whistle securely: SecureDrop

SecureDrop is an open source submission tool that can be installed by media organizations as a way to allow anonymous, secure submission of documents. Among the technologies and techniques it uses are Tor, GnuPG, Tails, and air-gapping, all discussed in this chapter.

Learning more

In an ideal world everyone would use encryption; in practice, however, it is beyond the technical skills, and patience, of most people. There have been a number of initiatives recently that seek to educate the broader public on cryptography issues.

Started when now-global **Cryptoparty** emerged practically overnight following an exchange on Twitter initiated from Melbourne, Australia. It aims to provide a space for those interested in learning about cryptography to learn from users who are already familiar with tools and concepts, through talks and workshops.