7.2 Operational Security

Operational security, often shortened to "opsec," is an important part of CVD operations. Opsec includes your ability to maintain security and confidentiality for information associated with vulnerability reports prior to disclosure.

PGP/GPG Key Management

Separate from the issue of maintaining encryption keys for your contacts, you must also maintain your own individual or organizational encryption key.

PGP/GPG is a form of asymmetric encryption that makes use of two different encryption keys called your *public key* and your *private key*. The public key is intended to be shared; you advertise your public key, and individuals or organizations wishing to contact you use your public key to encrypt a message. Messages encrypted to your public key can only be decrypted by the private key; therefore, it is important that your private key stays private, and that no one outside of your team or organization has access to this key.

A general discussion on encryption algorithms is beyond the scope of this report, but at the time of this writing, it is recommended to generate RSA keys with a length of at least 4096 bits to ensure security into the near-to-moderate-term future.

Use a Passphrase and Control Access

We recommend setting a strong passphrase on any key. Without a passphrase, anyone who obtains the key file can immediately use the key to sign messages or decrypt messages; if the private key is leaked to unauthorized users but a passphrase was applied, then the user would need to also know the passphrase before any damage could be done.

Of course, a persistent attacker could attempt to brute force the phrase, so ideally the private key should be kept somewhere safe, out of the hands of any unauthorized users. In other words, only members of the CVD team should know the passphrase or even have access to the key file. Ideally, if your CVD capability includes a dedicated communications team, restrict knowledge of the passphrase and access to the key material only to those members directly involved with communications. At the CERT/CC, we have implemented this by having dedicated systems for CVD communications work; private keys are only accessible from these systems. In this setup, users must specifically request access and can be allowed or denied based on need.

Use Revocation Certificates and Key Rotation

A concern is that the private key may land into unauthorized hands. This might occur in the event of a network breach, but another possibility is a disgruntled former employee retaining a copy of the key. Because of these possibilities, organizations using shared key material should generate a revocation certificate for their PGP/GPG key and store it somewhere safe. Obviously, it is important to restrict access to the passphrase and revocation certificate; typically, it should only be accessible by management. Should any emergency or security event occur, you can publish the revocation certificate to notify the public to not trust this key anymore. When a user imports your revocation certificate, it marks the associated PGP/GPG key as unusable and untrustworthy.

To further mitigate these concerns, we recommended that you rotate encryption keys (i.e., generate a new one) regularly. Some teams choose to use the same key for two, three, or more years without change. This recommendation arises to address concerns regarding the threat of network breaches and the potential impact of losing control of the private key. At the CERT/CC, we generate a new PGP/GPG key yearly.

Another reason to rotate keys is to revoke access to future encrypted email when analysts leave the CVD team. The best way to do this is to generate a new key whenever there are personnel changes; in this way, future messages will be encrypted to the new key with a new passphrase, and any former team members will be unable to access these messages even if they still have access to the old key.

Regardless of how often you generate a new PGP key, your latest PGP public key needs to be available to individuals and organizations so that they may contact you. Be sure your key generation process includes necessary steps to put your PGP public key in the public's hands. This can consist of posting your PGP public key directly to your organization website, or pushing your key to one of many PGP public key servers. You can use these same mechanisms to distribute your revocation certificate should the need arise.

Practical Tips for Key Management

We wrap up this discussion with a review of recommended practices for PGP/GPG key management:

- Generate an RSA key of at least 4096 bits.
- Restrict access to the private key material.
- Use a strong passphrase on the key.
- Restrict knowledge of the key passphrase to only those members of the CVD team involved in communications.
- Generate a revocation certificate for each key.
- Store the key passphrase and a revocation certificate in a safe location, such as a locked cabinet or safe in a secured area of the organization.

- Generate a new key whenever a member leaves the CVD team, and revoke the old key.
- Generate a new key periodically, regardless of other factors.
- Make your latest public key available in a known location to ensure recipients always have access to the latest key.

Handling Sensitive Data

Some of the information that passes through a CVD process may include information on an organization's internal processes, trade secrets, or even national security interests in some scenarios. Proper precautions need to be established. It is recommended that recipients treat all received data as private unless explicitly given permission to share.

Of course, there is some ambiguity when you say *private*: does that mean the information is for the whole organization? Just the CVD team? Possibly even a single analyst? In general, vulnerability information should be shared with the fewest number of people possible to effectively coordinate and remediate a vulnerability prior to disclosure. Clearly declaring the data's sensitivity can help to make that determination.

Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) has been adopted for a standards-track by FIRST [1]. By marking a document with a TLP level—Red, Amber, Green, or White—a sender can easily communicate the sensitivity of vulnerability information and expectations about sharing it further. In the context of CVD, the following applies:

- TLP:GREEN and TLP:AMBER are best suited for information shared between reporters, vendors, and coordinators during phases prior to public announcement of a vulnerability.
- If pre-publication announcements are made to deployers or other stakeholders, TLP:RED or TLP:AMBER could be a good fit.
- TLP:WHITE is most useful for public disclosures.

See Appendix B for more on TLP.

Don't Automatically Trust Reports

There are two reasons that organizations receiving vulnerability reports should maintain a degree of wariness regarding the reports they receive. The first is intentional misdirection of your CVD capability, which we already discussed in Section 4.3. The second is subtler, in that the technical infrastructure you deploy to manage CVD cases can potentially be affected by the vulnerabilities you are coordinating.

Vulnerability reports may contain hostile attachments—not necessarily as an attack, but simply a reporter sending a proof-of-concept for your review—so vendors and coordinators should design their report tracking systems and process accordingly. Be sure attachments to vulnerability reports are not opened automatically anywhere along the process. You might also institute a policy that such attachments are only to be opened within an isolated testing environment, not on production systems.

CVD participants should keep in mind that their case tracking and email systems themselves present attack surface and may be affected by the very vulnerabilities they are designed to coordinate. We have witnessed reports containing examples of image parsing vulnerabilities causing problems for both webmail and ticketing systems that automatically generate thumbnail previews of image attachments. Vendors and coordinators concerned about such risks should consider the degree to which their CVD support infrastructure is integrated with normal business operations systems. In some scenarios, maintaining parallel infrastructure may be preferable.

< 7.1 Tools of the Trade | 7.3 CVD Staffing Considerations >

References

1. FIRST, "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0," [Online]. Available: https://www.first.org/tlp. [Accessed 16 May 2017].