Information Leakage, Detection, and Prevention

By Wong Onn Chee

For many years, the focus of information security has been on the detection and prevention of intrusions. However, adequate measures must now be deployed to detect and prevent extrusions – compromises from within the organization.

Information leakage, detection and prevention (ILDP) is the new rising star in information security. For many years, the focus has been on the detection and prevention of intrusions. However, adequate measures must now be deployed to detect and prevent *extrusions* – compromises from *within* the organization.

The risks posed by extrusions are clear and significant, yet most organizations are hampered today by the lack of solutions or expertise in the area of ILDP. Below are just some of the common examples of information leakage:

- Employees leaked key bid information to competitors unknowingly
- CEOs lost laptops or USB storage devices while in transit
- Employees, who are leaving the organization, copied competitive information to their personal email accounts

More examples of data breaches can be found in the Chronology of Data Breaches of Privacy Rights Clearinghouse.[1] Many cases of information leakage go unreported due to fear of loss of confidence and regulatory penalties; hence, we are just looking at the tip of the iceberg.

Information leakage can be caused by negligence or intentional sabotage. Emails are unintentionally sent to the wrong recipients. Besides negligence, it is an universal truth that the motivation to leak sensitive information will exist no matter

what countermeasures your organization takes. And as storage media continually becomes more mobile and smaller in size, more sensitive information is likely to be stored on such media, having a greater likelihood of being lost or stolen. We have learned about information leakage incidents from history and we can be confident to see more of them in the future.

To help address ILDP, a new practical strategy is needed. This article will describe a new strategy consisting of five main components: Deterrence, Encryption, Forensics, Thin Clients and Identity Management.

Deterrence

In deterrence, the main focus is to increase the costs to potential perpetrators, making the information leakage unattractive. This is very similar to how the armed forces become a deterrence against potential intruders.

For deterrence to be effective, potential perpetrators must know there is a credible ILDP system in place. There is no point in building a great system if no one knows about it. This is akin to the regular demonstrations of military might that armed forces stage to inform the world of their capabilities. In information security terms, the following measures can be taken:

- Inform users that content in all information-related activities, such as Web surfing and copying to USB, within the organization belong to the organization, not to the users.

1   www.privacyrights.org/ar/ChronDataBreaches.htm.

37

- ○ **Food for thought:** In your organization, are employees being informed of the legal precedents supporting the ownership of content?

- Put up clear notices at all exit points informing employees about the presence of a ILDP system and the severe consequences if caught.

  - ○ **Food for thought:** In your organization, is there a notice to inform employees about their responsibility whenever a USB storage device is attached to their corporate workstations?

- Send summary information of employees' usage to remind them that their activities are monitored and make them think twice before leaking information.

  - ○ **Food for thought:** In your organization, do you publish the top users of emails, web traffic and USB storage connections on a regular basis?

- Impose heavy penalties for information leakage offences. Put greater emphasis on the criminal penalties which have a stronger deterrence effect. For key appointment holders, a security bond can be imposed and should be accepted in writing.

  - ○ **Food for thought:** In your organization, are users required to sign security bonds that sets a minimum penalty that is high enough to be a deterrent in the event of information leakage?

- Inform employees of the ILDP system and the related civil/criminal penalties when they join your organization.

  - ○ **Food for thought:** In your organization, does your employee handbook state clearly the penalties for information leakage?

Though the presence of a ILDP system should be made known, the actual configurations or detection rules should remain secret. This is for the same reasons why armed forces maintain confidentiality about the actual configurations used for their publicly-known weapons systems. If they know *how* they are being monitored and *what* is being monitored, potential perpetrators will find means to bypass and evade detection.

Current popular measures can also deter or prevent information leakage. These measures include removal of administrative rights to prevent installation of applications that pose information leakage risks and dual control of administrative passwords.

Finally, for the ILDP system to be credible, an effective forensics environment must be in place. Without proper forensics, perpetrators may go free even if information leakage is detected. Forensics will be discussed in more detail in a separate section.

Encryption

In encryption, the main focus is to prevent unintentional leakage through theft or negligence. Note, however, that encryption does not prevent intentional leakage by authorized users. There are three main areas where encryption is useful: Network, Endpoint and Content.

Network encryption

Network encryption is the most prevalent among the three. It can take the form of SSL-encrypted web traffic, encrypted SSH access to Unix systems, VPN remote access and many others.

Endpoint encryption

Often removable storage devices and notebooks are found lying around without any supervision or physical restraint. With endpoint encryption, the storage media is protected with strong encryption to ensure that only the authorized users can access the information. With growing prevalence of mobile computing devices, the need for endpoint encryption is much higher than before.

Content encryption

Content encryption is a commonly neglected safeguard. Content encryption offers better protection than endpoint encryption because the protection is independent of the storage media. Coupled with secure authentication, such as two-factor or biometric authentication, content *and endpoint* encryption can effectively eliminate the risk from unintentional leakage through theft or negligence.

However, there have been several misconceptions which are holding back the wider adoption of endpoint and content encryption:

- **Encryption is costly** – Though encryption does come with additional costs, one has to weigh against the value of information it is protecting. No one will question the economics of spending thousands of dollars to protect the information on a CEO's notebook which may be valued at millions of dollars. Furthermore, the cost of encryption has fallen over time with more efficient algorithms being developed.

- **Following standards and rules ensures information protection** – This is a common folly still committed by organizations today. No matter how stringent the standards or rules are, we are still human. Humans are prone to lapses and may become negligent. This is especially so for a CEO who has been in the air every day of the week. In addition, internal standards and rules cannot deter or prevent physical theft by external parties.

- **Encryption requires expensive storage** – With the development of newer, more efficient encryption algorithms, the storage requirements for encryption has fallen. In addition, with the advancement in stor-

age technologies, the unit storage cost has fallen to render this point immaterial.

- **Encryption reduces performance** – It is true that encryption does consume computing power and imposes a performance penalty. However, with the availability of hardware-based encryption accelerators, encryption can be performed concurrently without material impact to the business workload. Furthermore, with the development of more efficient algorithms, keys of shorter length can offer similar, if not better, encryption than before. In most cases, the performance penalty imposed by encryption should not exceed 5%.

Forensics

In forensics, the main focus is to build a credible detection capability and provide legally-submissible evidence. Regardless of how advanced our protection systems are, a good forensics system is required for accurate detection and effective follow-up actions. Without proper forensics, you may find your ability to carry out corrective actions, such as imposing penalties or reporting to authorities, to be severely limited. A common mistake is to think that blocking access removes the need for a good forensics system.

Three most common shortcomings in forensics are:

- **Insufficient logging** – Most companies do not log the content of information being sent out via removable storage and web-based email. Many a time, you hear organizations relying on "trust" that their users will not leak sensitive information.

- **Improper handling of digital evidence** – This is not surprising as most information security professionals are not trained in the procedures of what constitutes legally-submissible evidence and how to handle evidence when it is collected. No matter how accurate the detection system is, evidence, once tainted by improper handling, will be rendered useless.

- **Case mismanagement** – Often escalations of information leakage are not properly managed. Most organizations, especially in Asia, do not provide an independent escalation path for the whistle-blowers. Examples include premature alerting of the perpetrator and lack of anonymity for the whistle-blower.

A comprehensive ILDP system must possess good forensics capabilities at the network and endpoint levels. For the network level, the forensic component of the ILDP system should be passive and run in an out-of-band (OOB) network. It must be able to perform analysis of the voluminous network traffic and not be just a "dumb dump." The obvious challenges in network-based forensics are in the large volume of data and the presence of encrypted network traffic. For the endpoint level, the forensic component should be passive and not easily identifiable by users. Compared to network-based forensic solution, the advantages of an endpoint forensic solution include the ability to monitor for execution of unauthorized

programs and capture information before it is encrypted over the network.

Thin Clients

Thin clients can be used to achieve greater endpoint security. Some thin clients come with no local storage, reducing the number of storage media to protect. Others come with a minimal locked-down local storage which prevent users from modifying any local content. However, for the later, endpoint encryption should be considered as well for a comprehensive protection.

Use of thin clients requires some form of centralized server computing environment, allowing you to monitor and detect information leakages from centralized points. Thus, with thin clients you can better manage the environment of remote offices or branches in order to detect and prevent information leakage.

Finally, most, if not all, thin clients come with the capability to lock down their support for external storage devices, hence, effectively preventing leakages via external devices.

Identity management

Identity management is extremely important. All the above components will fail if user identities are stolen and misused. Coupled, with proper authentication, authorization and auditing, identity management helps to prevent identity theft. With proper identity management, you can achieve an timely management of identities in the critical systems in your organization. How many times have we heard of orphaned user accounts remaining in critical systems after users left the organization? Timeliness is critical as any unused account provides an opportunity for a perpetrator to obtain and leak information.

Coupled with secure, non-repudiable authentication, identity management can provide an automated, self-service approach to password management, which in turn can help reduce the opportunities for social engineering and theft of identities.

About The Author

Onn Chee is currently working as the Chief Technology Officer in Resolvo Systems, a leading open standards infrastructure firm in Singapore. He has led numerous large-scale projects, primarily in the government and defence sectors. His areas of expertise include IT infrastructure and security strategy, information security management, identity management and network security. Onn Chee is a founding member and the first Vice-President of the Information Systems Security Association (ISSA), Singapore Chapter and current Singapore chapter president of Open Web Application Security Project. He may be reached at ocwong@usa.net.