CPNI
Centre for the Protection of National Infrastructure

CPNI VIEWPOINT 01/2009

HARDWARE KEYLOGGERS

MAY 2009

Acknowledgements

CPNI would like to acknowledge and thank Context Information Security Ltd for their help in the preparation of this report. The findings presented here have been subjected to an extensive peer review process involving technical advisers from both CPNI and wider industry.

Executive summary

Keyloggers represent a viable threat to organisations and to individuals. Their design is to record all keystrokes entered on the keyboard into a system, allowing an attacker access to those keystrokes.

Hardware keyloggers, unlike software, are highly targeted, as they require equipment to be physically placed on or in a computer, keyboard or KVM. This means that they must either be supplied already fitted as part of the supply chain or installed by an individual who has physical access to the computer.

Hardware keyloggers are generally undetectable by software tools. This leaves physical protection as the only viable defence and there are a number of physical defensive options. Although none constitute a single simple solution, there are various measures that can be adopted depending on the level of protection required. It is also recognised that not all computers require the same level of protection. It is strongly recommended that a risk assessment is carried out to determine the criticality of computers and terminals, and the results of this assessment used in a layered approach according to the criticality of the computer.

Wireless devices, such as wireless keyboards and wireless KVMs, pose an increased risk. These devices are prone to interception, as they actively broadcast their signal over the air. The protection used for most of these wireless devices is not sufficiently strong to prevent anything more than casual eavesdropping. However, there appears to be no commercial equipment on the market to exploit this vulnerability.

There are three categories of mitigation option:

- Preventing installation
- Detecting installation
- Limiting impact

For computers that need high levels of protection, it is recommended that they are placed within a physically secure area with zoned access control, and access restricted to a specific set of vetted staff. Additional options that should be considered include:

- The introduction of a secure physical enclosure for the computer and its connections — this helps to protect the keyboard connector and internals of the computer from tampering.
- The use of tamper evident seals on the keyboard and any attached KVM to deter unauthorised modifications and ensure that visual evidence exists where tampering has occurred.
- Sourcing computer equipment from suppliers who have been subject to a comprehensive due diligence process.

- Completing regular visual inspections of systems to ensure no keyloggers have been attached.
- Performing regular bug sweeps and RF detection scans as part of the vulnerability assessment process.
- The use of front mounted USB ports for keyboard and mouse, to make visual inspections easier.
- Removing converters that convert between USB and PS/2 connections, as this could provide a potential installation place for keyloggers.

Capabilities

There are many different forms of keyloggers available on the open market. The majority of keyloggers identified were below the £150 mark to purchase. Only four keyloggers were found exceeding this price point. Keyloggers were found to be available to suit just about any need, with storage capacities exceeding the levels that an average computer user would enter in a month. A few keyloggers support wireless technologies such as Bluetooth. This level of functionality makes keyloggers a formidable tool in obtaining information from an organisation.

Features of these keyloggers include:

- Easy to fit external USB and PS/2 models
- Small footprint to make detection harder
- Internal models that are hidden inside the computer or keyboard
- Keyboards with internal keylogger already fitted
- Large numbers of keystrokes logged (in excess of millions of keystrokes)
- The ability to record the date and time of when keystrokes were made
- The use of AES encryption to protect keystrokes recorded
- The use of wireless technologies to allow remote retrevial without exposing the operative to the risk of discovery trying to recover the device.

Traditionally, a keylogger has required the operative to retrieve the device in order to obtain the data stored on it. However, wireless technologies such as Bluetooth have been integrated to allow for remote retrieval of the information stored. Such a keylogger could remain in place for a long period of time, without detection.

Although research was performed, no commercial wireless keyboard sniffers were identified on the open market.

Associated risks

Keyloggers, by design, are intended to capture information entered at the keyboard and make it available to a third party.

Stolen user credentials

Typically the information desired is in the form of user credentials, such as usernames, passwords and personal identification numbers (PIN).

The information captured could then be used to perform operations such as establishing a connection to a virtual private network (VPN) or authenticating with systems or web sites with the user's credentials.

Where cryptographically protected material is in use, the information captured may represent a user's PGP or Hushmail passphrase. Alternatively it may represent the key to an encrypted hard disk, or an SSL certificate.

Wireless keyloggers offer the ability to capture and transmit keystrokes as they are entered, revealing one time or time synchronised passwords, such as RSA's SecureID tokens, and potentially providing a suitable time window in which such keystrokes could be used.

Business information

Keyloggers are also capable of collecting other information. This could include financial account details, where formatting of data makes it easier for a program to identify the relevant part of the data.

Information can also be garnered about web sites visited and search requests made to search engines. This can provide a view into what a user is searching for. Combining this with other activities that a user may be performing can provide insight into the type of information that a user is working with.

Behaviour

Similarly, composing an email or other document would require the use of a keyboard. This information can be gathered and examined in order to reconstruct the text that was typed. This can provide a highly detailed view into what is happening inside an organisation.

Mitigating risk

Prior to attempting any mitigating actions, it is important that a risk assessment is carried out in order to determine the criticality of PCs and terminals across the domain. This will identify those that are most critical. It is also recommended that a Personnel Security Risk assessment is performed. The following documents available from the CPNI website offer guidance:

- “Risk Assessment for Personnel Security – a guide” and associated training course “Risk Assessment in Personnel Security”
- “Personnel Security: Threats, Challenges and Measures”
- “Ongoing Personnel Security: a good practice guide”

Mitigation should be applied in a layered approach according to the criticality of the PC.

There are three major methods for mitigating risk, in order of preference:

- Preventing installation
- Detecting installation
- Limiting impact

Where possible, the first two methods should be implemented as part of a security in depth methodology.

Preventing installation

The recommended options for preventing installation are:

- Physical access – Placement of computers within a physically secure area, protected by physical controls such as locked rooms, together with personnel controls such as zoned access control. This limits access to sensitive computers to authorised individuals.
- Trusted sourcing – Sourcing computer equipment from suppliers who have been subject to a comprehensive due diligence process.
- Physical enclosure – The introduction of a secure physical enclosure protecting the computer or KVM and its connections. This helps to protect the keyboard connectors and internals of the computer or KVM from interference.
- Deterrence – Deterrents such as CCTV, regular security guard patrols and logging for all staff who have access to sensitive areas. Security guards should be trained to be aware of the types of activity that is related to keylogger installation and retrieval.

Detecting installation

The recommended options for detecting installation are:

- Visual detection – Visual inspection of systems (computers, keyboards and KVM switches) in order detect the presence of external keyloggers. Internal keyloggers are likely to only be detected by staff trained in visual inspections of the internals of systems. See page 7 for examples of keyloggers.
- Front mounted keyboard/mouse ports – The use of front mounted USB ports for keyboard and mouse, in order to make visual inspections simpler to carry out.
- Tamper evident seals – Tamper evident seals on the keyboard, KVM and computer can be used to detect attempts to tamper with the internals. These seals are designed to leave residue should any attempt be made to remove them.
- Case intrusion alerts – Case intrusion alerts, warn a central monitoring system if the case is removed from a computer. This also requires the BIOS to be suitably locked down.
- Bug sweep/RF detection sweep – Performing a bug sweep with RF detection can provide a mechanism for detecting some kinds of wireless keyloggers. However, other types are significantly more difficult to detect.
- Limited expansion capability for laptops – Filling the miniPCI slot limits the places that a keylogger can be placed on a laptop. All laptop keylogger designs examined used the miniPCI slot.
- Not using converters to convert between PS/2 and USB, as these could make it more difficult to detect the use of a keylogger. However, no keyloggers posing as such a converter were identified on the open market at the time research was carried out.

Limiting impact

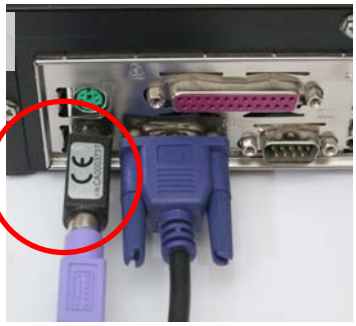
In a limited set of circumstances, the sensitive data that is entered may only be a password or PIN. In these cases, it may be more effective to protect just the access credentials, rather than trying to protect all data that is entered via the keyboard. These methods are:

- Use of two factor authentication to protect credentials, as long as one of the factors is not entered via the keyboard.
- Using a virtual keyboard, so that information is not entered on the physical keyboard. This has risks, including shoulder surfing, as well as disability discrimination for visability impaired users.

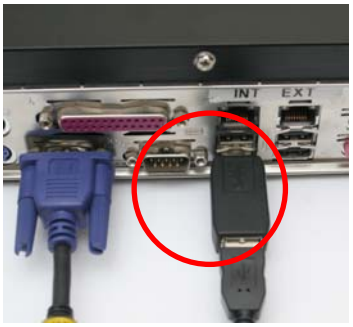
Examples of keyloggers

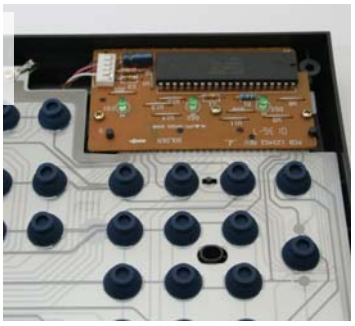
1. 

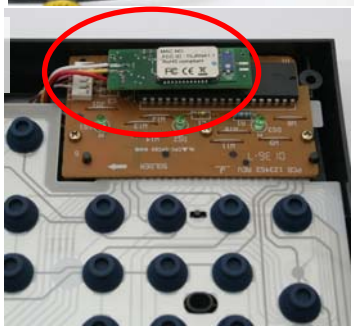
2. 

3. 

4. 

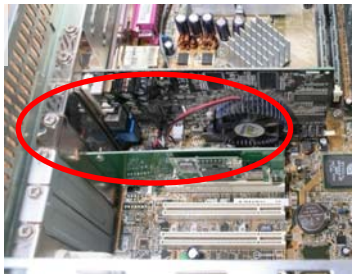
5. 

6. 

7. 

8. 

9. 

10. 

11. 

12. 

13. 

1. PS/2 System
2. PS/2 system with KeyKatch
3. PS/2 system with KeeLog
4. USB system
5. USB system with KeeLog
6. Keyboard controller
7. Keyboard controller with wireless keylogger
8. Top of wireless keylogger
9. PCI expansion slots
10. PCI expansion slots with KeyCarbon Raptor
11. KeyCarbon Raptor mini-PCI card on PCI carrier
12. MiniPCI expansion slot on Laptop
13. MiniPCI expansion slot with KeyCarbon Raptor