Device Management Technology for Preventing Data Leakage

● Jun Sugii ● Keita Nojiri

Security countermeasures against targeted attacks are important elements in preventing the leakage of data such as critical internal company data and customer data. Targeted attacks often focus on known vulnerabilities, making it essential to apply security patches in a timely fashion. However, making sure that security patches are applied to all devices is no easy feat. Even if security patches are applied in a thorough manner, this will not guard against zero-day attacks that target unknown vulnerabilities. That makes it vital to implement security countermeasures which prevent data from being leaked even in the event of malware infection. Fujitsu provides FUJITSU Software Systemwalker Desktop Patrol (DTP) and FUJITSU Software Systemwalker Desktop Keeper (DTK) to solve this problem. DTP is used to centrally manage information and communications technology (ICT) assets and control security. DTK almost completely eliminates the risk of data leaks by applying operation restrictions to ICT assets and logging ICT asset usage. This paper introduces DTP and DTK, which prevent data leakage from endpoint devices (computers, virtual terminals, and smart devices).

1. Introduction

Using information and communications technology (ICT) and connecting to internal and external networks have now become a common part of the business operations of enterprises. They must therefore take measures to prevent being infected with viruses via these networks, which makes it essential to install anti-virus software.

However, targeted attack approaches, such as spoofing e-mail senders and sending virus-bearing attachments, or spoofing actual websites to get users to download executable files, are constantly evolving. Zero-day attacks, which use undiscovered vulnerabilities, cannot be guarded against by installing anti-virus software alone.

This paper introduces Fujitsu's approaches for using central management of ICT assets to automatically and forcibly apply security patches and prevent the leakage of information via e-mail or the Web from endpoint devices (computers, virtual terminals, and smart devices).

2. Issues with information leakage prevention

The following four challenges need to be surmounted in order to prevent information leakage.

1) Control of ICT assets

Company system administrators (hereafter referred to as "administrators") must be aware of all ICT assets in order to ensure compliance and appropriate ICT investment; in addition, they must also maintain security. Ledgers such as Microsoft Excel spreadsheets are used to manage ICT assets.

In the past, pieces of hardware such as servers and computers have been expensive, so companies have used them continuously over a number of years. Hardware additions and replacements were also performed roughly once per year. Software updates, such as new security patches issued by software vendors or the addition of new functions, were infrequent. This meant that hardware and software ledgers did not need to be updated often, allowing administrators to manage ICT assets by manually updating ledgers. However, hardware, such as computers, hard disk drives (HDD), and removable high-capacity media, has become far less expensive than it once was, while hardware performance has grown by leaps and bounds, resulting in a rapid rise in the frequency with which companies replace hardware. The ways in which ICT devices are used in business have also changed. Pieces of hardware such as servers and computers are being replaced by virtual devices and smart devices. The growing volume of attacks targeting vulnerabilities has also produced a rapid rise in the frequency with which security patches are applied and new functions are added. Accompanying this rapid rise in the frequency at which both hardware and software updates are applied, the ability to update ICT asset ledgers on a real-time basis is becoming an important part of managing corporate systems that are made up of various ICT assets. Manual updating of asset ledgers by administrators has become difficult to achieve.

This has made it essential to introduce asset management tools which can reduce the asset management workload placed on administrators while automatically managing large systems.

2) Defense against attacks aimed at known vulnerabilities

Many targeted attacks are aimed at known vulnerabilities in operating systems, Web browsers, and the like. Applying the latest security patches to all company ICT assets in a timely fashion is therefore key to preventing information leakage. Companies have a wide range of ICT assets, so it is necessary to achieve the control described in 1) above to manage the status of security patch application.

3) Defense against attacks aimed at undiscovered vulnerabilities

Applying the latest security patches is not sufficient to defend against zero-day targeted attacks, which use undiscovered vulnerabilities. It is therefore important to prevent information from leaking even in the event of a malware infection. Doing so requires the ability to control user devices, such as controlling user operations on the device and disconnecting specific devices from the network.

4) Prevention of information leakage via removable media

Improvements to ICT environments have created more efficient work styles which are not dependent on either time or location, making it possible to work not only in the office, but also from outside the office and at home. This has created more situations in which important company data, customer information, and the like are stored on USB flash drives, removable HDDs, or other removable media and used outside the office. Removable media is also used to store large amounts of data which cannot be sent by e-mail. However, there has also been a rise in recent years in the number of companies and individuals that purchase personal information, and an unending stream of incidents in which employees or other related parties steal internal personal information. The increased popularity of smart devices, and the use of personal smart devices as removable media, has made it easier than ever to take important data and customer information outside of companies.

The frequency with which removable media is used has risen, and so has the variety of removable media types, so the risk of information leakage remains high. Preventing these leaks requires the ability to prevent removable media from being brought in or out of the office, and the ability to restrict its usage scope. It also requires the ability to record individual operations performed by users to track information leakage routes when problems occur.

Fujitsu developed and released FUJITSU Software Systemwalker Desktop Patrol (DTP)[1] and FUJITSU Software Systemwalker Desktop Keeper (DTK)[2] in order to solve these four challenges.

The rest of this paper explains the measures this product uses to tackle these issues.

3. Security control through centralized management of ICT assets

DTP performs centralized management of ICT assets such as servers, computers, virtual devices, and smart devices, providing security control of ICT assets (**Figure 1**). It can automatically defend against targeted attacks that aim for known vulnerabilities by performing computer security control, automatically distributing and applying security patches, and specifying prohibited software.

The functions used to achieve this are described below.

1) Understanding of software installation status

DTP automatically collects information about software which has been installed on computers and smart devices. This makes it possible for administrators

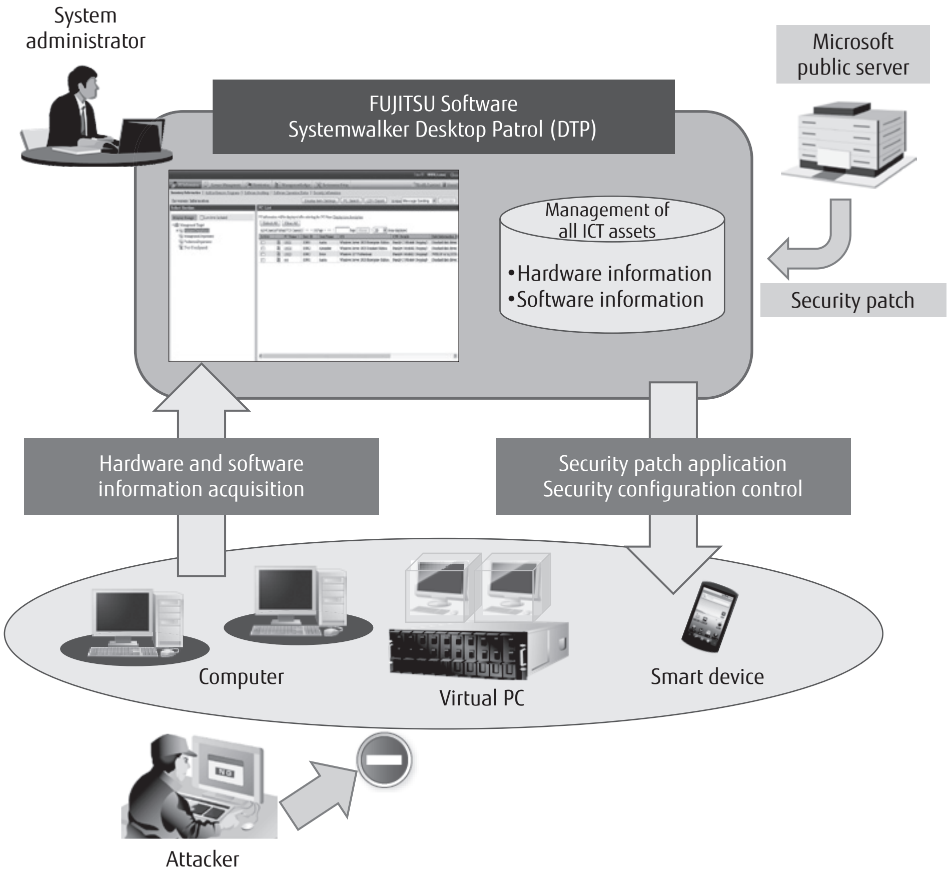
System administrator
FUJITSU Software
Systemwalker Desktop Patrol (DTP)
Microsoft public server
Management of all ICT assets
•Hardware information
•Software information
Security patch
Hardware and software information acquisition
Security patch application
Security configuration control
Computer
Virtual PC
Smart device
Attacker

Figure 1
DTP overview.

to centrally manage software assets used in the company. DTP also automatically acquires the necessary information regarding the status of anti-virus software installation and security patch and virus definition file application, making it possible to assess conditions on both an individual-division and individual-device basis.

2) Timely application of security patches

Security patches issued by Microsoft are received from public servers and can be automatically applied to computers (**Figure 2**). This automatic patch application greatly reduces the downloading and application workload placed on administrators. It also prevents devices from going unpatched, ensuring greater security.

3) Security configuration auditing and control

DTP can audit whether individual computers are in compliance with security policies set by administrators (**Figure 3**). When policy infractions are detected, warnings can be displayed on the screen of the computer in question, indicating countermeasures to be implemented, and if no corrective measures are taken, administrators can make changes themselves. DTP also provides the ability to collect and audit security information for smart devices. This makes it possible for administrators to gain an overview of all corporate ICT asset security information for computers and smart devices.

4. Information leakage risk management

DTK almost completely eliminates the risk of information leakage through its functions for prohibiting specific operations by computers and smart devices, recording operations, and analyzing logs (**Figure 4**). It can automatically defend against zero-day attacks by prohibiting operations on computers and smart devices, and automatically disconnecting specific devices from networks. It can also limit the carrying out of various types of information via removable media,

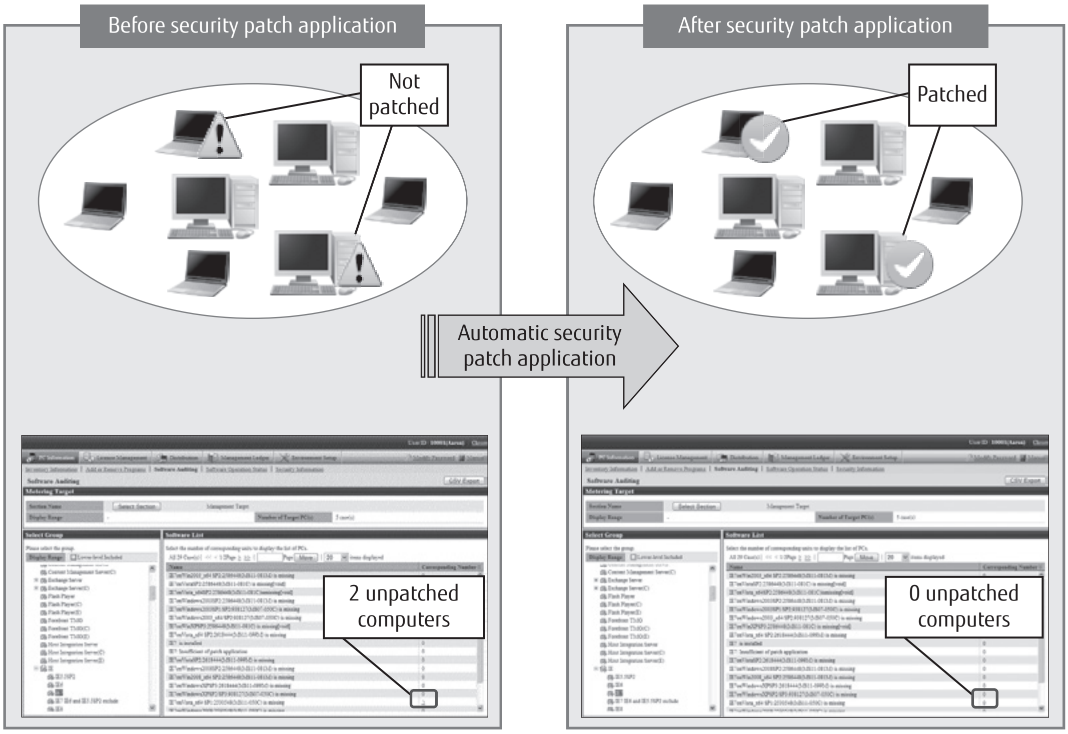
Before security patch application
Not patched
After security patch application
Patched
Automatic security patch application
2 unpatched computers
0 unpatched computers

Figure 2
Security patch application.

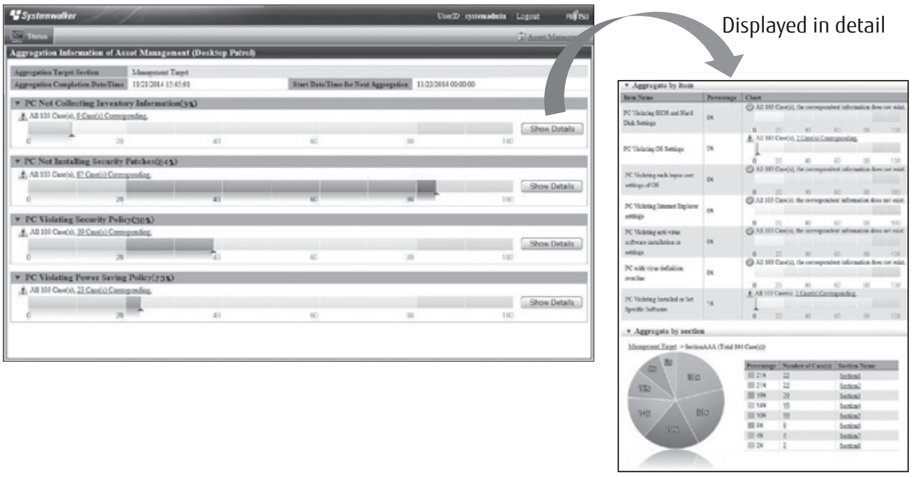
Systemwalker
UserID : systemadmin
Logout
Status
Aggregation Information of Asset Management (Desktop Patrol)
Aggregation Target Section
Management Target
Aggregation Completion Date/Time
11/21/2014 15:45:40
Start Date/Time for Next Aggregation
11/22/2014 00:00:00
PC Not Collecting Inventory Information(9%)
All 100 Case(s), 9 Case(s) Corresponding.
PC Not Installing Security Patches(84%)
All 100 Case(s), 87 Case(s) Corresponding.
PC Violating Security Policy(38%)
All 100 Case(s), 39 Case(s) Corresponding.
PC Violating Power Saving Policy(23%)
All 100 Case(s), 23 Case(s) Corresponding.
Show Details
Displayed in detail
Aggregate by item
Aggregate by section

Figure 3
Security configuration auditing.

networks, and the like, and can track leakage routes by using records and collected logs. These help prevent information leakage via removable media.

The functions used to achieve this are described below.

1) Restriction functions

Administrator-defined restriction policies can be used to prevent computers and smart devices from performing operations such as those below (**Figure 5**).

- Exporting or importing data to/from removable media such as USB flash drives or smart

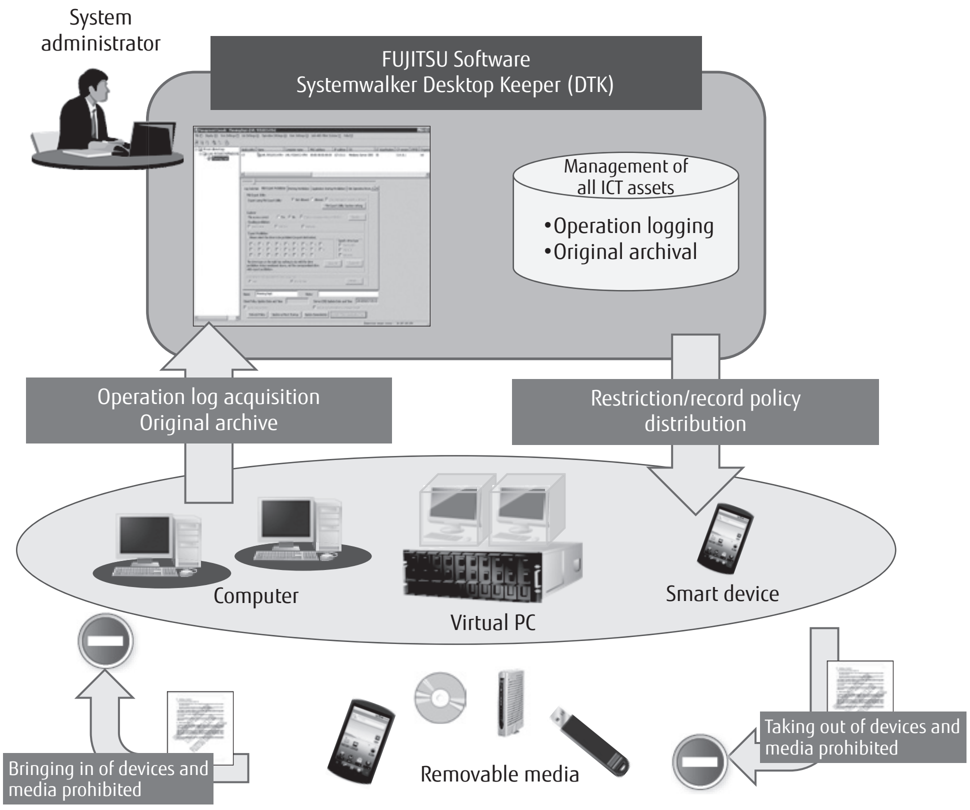
System administrator
FUJITSU Software
Systemwalker Desktop Keeper (DTK)
Management of all ICT assets
•Operation logging
•Original archival
Operation log acquisition
Original archive
Restriction/record policy distribution
Computer
Virtual PC
Smart device
Bringing in of devices and media prohibited
Removable media
Taking out of devices and media prohibited

Figure 4
DTK overview.

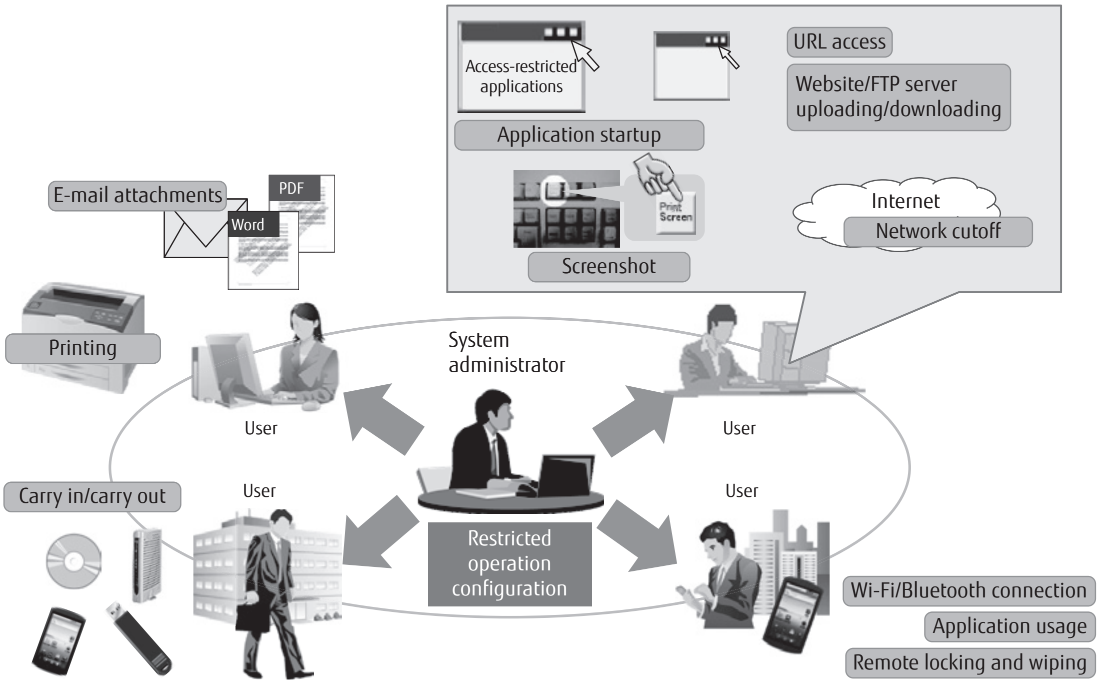

Figure 5
Restriction functions.

devices[note)]
- Uploading or downloading files using FTP (file transfer protocol) servers or websites
- Printing out of information
- Transmitting files as e-mail attachments (unencrypted files)
- Screenshots of information displayed on-screen
- Use of unauthorized applications
- Logging in using a user ID with administrator permissions
- Connecting to inappropriate networks
- Wi-Fi/Bluetooth connection of smart devices
- Inappropriate operation of smart devices which have been stolen or lost (remote locking or wiping of smart devices)

2) Recording functions

Both prohibited and permitted operations can be logged. The following operations can also be logged.
- Web access, SD card or SIM (subscriber identity module) card mounting/unmounting, and placing/receiving of telephone calls on smart devices
- Computer logon/logoff, computer startup/shutdown/sleep/wake
- Viewing and creation of files
- Drive allocation by mounting of USB flash drives, etc.
- Original archive when exporting files

3) Log analysis functions

Log analysis can be broadly broken down into the following three categories.
- Information leakage prevention diagnostics

DTK tabulates logs from the previous day and displays tabulation results of operation logs for individual devices for the previous one-week period. This information can be used to quantify trends related to operations which can lead to information leakage and assess risk propensity.
- Tabulation by purpose

Risk propensity can be analyzed for each operation with potential for information leakage. Various conditions can be set for already collected logs, such as tabulation unit and period, and then aggregation can be performed.
- Log tracing

Log viewer search results can be used to track the operation histories of specific users, making it possible to investigate if they have engaged in any risky behavior, such as accessing inappropriate networks.

5. Conclusion

This paper introduced FUJITSU Software Systemwalker Desktop Patrol (DTP) and FUJITSU Software Systemwalker Desktop Keeper (DTK), which make it possible to in advance prevent information leakage through device asset management and security countermeasures.

In the future, companies will continue expanding globally, and further implement Bring Your Own Device (BYOD) policies. In order to respond to these changes, we plan to realize centralized management of various countries' ICT assets and secure device management in which corporate and personal data (or applications) are separated. Fujitsu will use the technologies it has developed through its asset management and security management experience to supply middleware which takes advantage of cutting-edge technologies.

note) Supports file transfer methods (PTP/MTP) on the latest smart devices, as well as file copying via iTunes on iOS devices.

References

1) Fujitsu: FUJITSU Software Systemwalker Desktop Patrol (in Japanese).
http://systemwalker.fujitsu.com/jp/desktop_patrol/

2) Fujitsu: FUJITSU Software Systemwalker Desktop Keeper (in Japanese).
http://systemwalker.fujitsu.com/jp/desktop_keeper/

Jun Sugii
Fujitsu Ltd.
Mr. Sugii is currently engaged in development of ICT asset management software.

Keita Nojiri
Fujitsu Ltd.
Mr. Nojiri is currently engaged in development of ICT asset management software.