Cyber Attack Countermeasures Based on WebSAM IncidentGuard and Authentication Switches

EBATA Kazumasa, WATANABE Youko, NEZU Yuichirou, TANIMURA Satoru

Abstract

Some of the special characteristics of recent virus/worm infections are that they feature a very high infection potential that can result in a rapid spread of infection damage, and this situation has led to an increased need for new countermeasures against the spread of virus infections. In the part, our network security product WebSAM IncidentGuard has been providing virus infection spread countermeasures in a tie-up with security devices within the framework of NEC's cyber attack countermeasures. As this product has recently been upgraded to enable compatibility with IEEE802.1X compliant authentication switches, it has now become possible to propose stronger, double cyber attack countermeasures, with which the authentication switches prevent unauthorized connection while IncidentGuard prevents viruses from being spread during operations after connection. This paper is intended to outline the improved effects of the current upgrade.

Keywords

cyber attack countermeasures, IEEE802.1X authentication

1. Introduction

Infections of viruses/worms have recently been causing serious damage to an increased number of businesses by shutting down their networks, including fundamental job systems. It is now an urgent matter for businesses to adopt adequate cyber attack countermeasures in order to prevent loss of profits.

The mainstream traditional solution against cyber attacks functions as a quarantine network system; when connecting client PCs, the system temporarily isolates the client PCs that are unauthorized or of a low security level, makes them safe by applying a security patch, etc., and then permits their connection to the job network.

However, recent viruses/worms often take the form of e-mail bourne viruses, etc. They are very strongly infectious and the infections extend all over the network in a very short time and before a security patch can be provided. Consequently, it is critical to take countermeasures against such attacks during operations after connection, besides those that are taken at the time of the network connection.

2. Explanation of Previous Functions

2.1 Connection Port Search/Shutdown Function

WebSAM IncidentGuard (hereinafter referred to as IncidentGuard) is one of the NEC's cyber attack countermeasure software products, used to isolate virus-infected client PCs from the network. Introducing IncidentGuard with security devices makes it possible to prevent viruses from being spread.

The traditional functions provided by IncidentGuard are the function to search the connected switch port based on the IP address of the PC suspected of being infected by a virus, which is contained in the security event data from the security devices, and the function to shut down the searched port. The search and shutdown operations are performed manually by the operator in the event of receiving any security event from security devices.

The specific flow of processing is as described below and in **Fig. 1**.

① On receipt of a security event from security devices, the system identifies the IP address of the host to be searched.

② The system inquires the IP address tables in the L3 switches in the network, identifies the L3 switch in the same network as the IP address of the search target host and identifies the MAC address of the search target host from the ARP table of the L3 switch.

③ Based on the connection port information obtained from the MIB corresponding to the MAC address tables for the switches (Bridge-MIB) and neighbor information obtained from the discovery protocol, the system obtains the position relationship between the switches and identifies the switch and port to which the search target host is directly connected.

④ The system rewrites the value of the MIB (ifAdminSta-

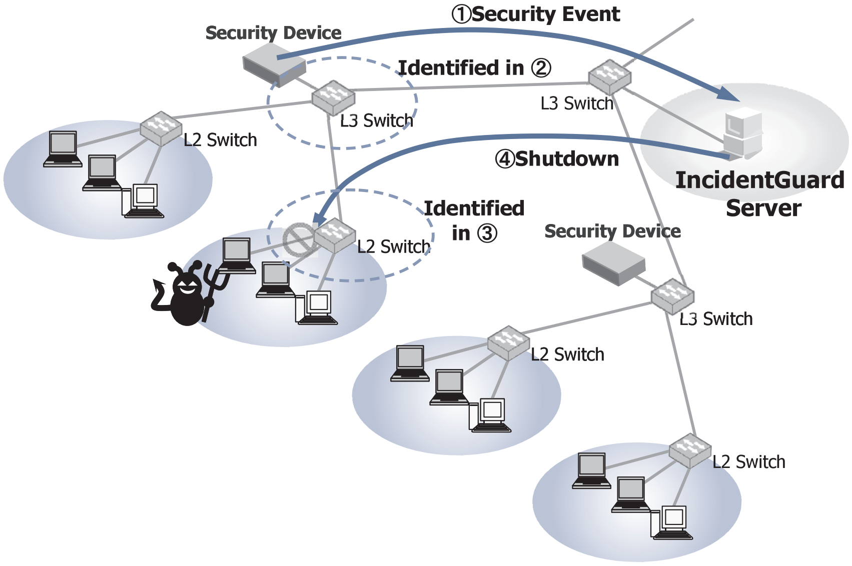

Fig. 1 Diagram showing operation of IncidentGuard.

tus), which is used to control the port setting status, of the switch port identified in ③ in order to set the port to the link-down status.

As this method references the Bridge-MIB in order to identify the port, it is called the Bridge-MIB search method.

2.2 IEEE802.1X Authentication Function

The IEEE802.1X authentication function is used as an authentication check when a client PC attempts to connect to a network. The IEEE802.1X compliant authentication switches (hereinafter referred to as “authentication switches”) such as the UNIVERGE QX series switches make it possible for the network to authorize access only for pre-registered users.

The specific flow of the authentication processing procedure is as described below and in **Fig. 2**.

① The client PC is connected to the authentication switch (Authenticator).

② The user inputs the user authentication information in the supplicant

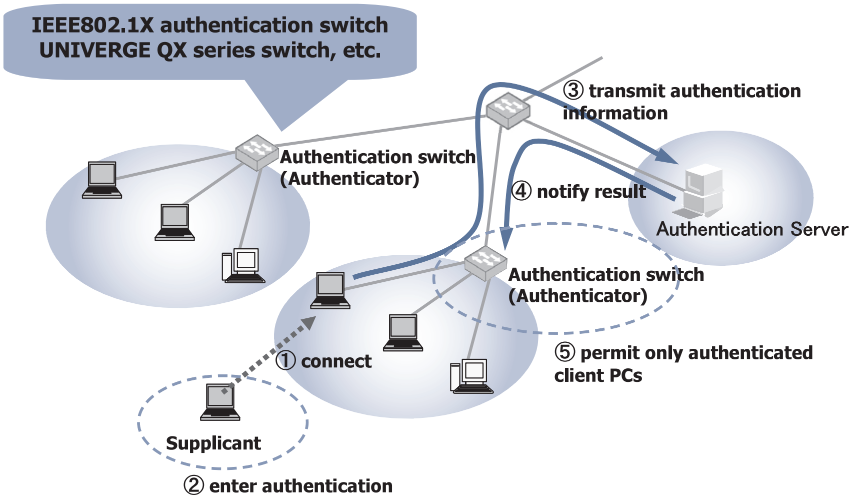
IEEE802.1X authentication switch
UNIVERGE QX series switch, etc.
③ transmit authentication information
Authentication switch (Authenticator)
④ notify result
Authentication Server
Authentication switch (Authenticator)
① connect
⑤ permit only authenticated client PCs
Supplicant
② enter authentication

Fig. 2 Flow of the IEEEE802.1X authentication.

- IEEE802.1X-compliant supplicants (client software)
- The client is the supplicant in the IEEE 802.1X specification.
- Authenticators and supplicants communicate with one another) of the client PC.

③ The user authentication information is sent to the authentication server.

④ The result of authentication by the authentication server is sent to the authentication switch.

⑤ The authentication switch controls the network access of the client PC according to the authentication results.

3. Function Enhancements Resulting from the Present Upgrade

3.1 Search Method Expansion

The authentication switch holds an IEEE802.1X authentication MIB, which contains information as shown in **Table** below.

As a result of the present development the search function of IncidentGuard has been upgraded in order to enable searches based on the IEEE802.1X authentication MIBs. This provides improved search accuracy in addition to the traditional Bridge-MIB search method. This new method is called the IEEE802.1X authentication MIB search method.

In the IEEE802.1X authentication MIB search method, the processing for identifying the MAC address from the IP address of the search target is the same as before, but the processing for identifying the switch port to which the client PC having the search target MAC address (③ in Section 2.1) has been modified as described in ③' below.

Table IEEE802.1X authentication MIB (Partial).

Items		Details
1	Name	dot1xPaeSystem.dot1xPaeSystemAuthControl
	Description	Status of the use of the IEEE802.1X port access control function of the entire device. enable(1), disable(2)
2	Name	dot1xPaeAuthenticator.dot1xAuthConfigTable. dot1xAuthConfigEntry.dot1xAuthAuthControlledPortStatus
	Description	Current IEEE802. IX authentication status of the port. authorized(1), unauthorized(2)
3	Name	dot1xPaeAuthenticator.dot1xAuthStatsTable. dot1xAuthStatsEntry.dot1xAuthLastEapolFrameSource
	Description	MAC address of the last IEEE802.IX authenticated client PC at the port.

*The MIB names in this table are described based on the following MIB tree:
iso.std.iso8802.ieee802dot1.ieee802dot1mibs.ieee8021paeMIB.paeMIBObjects.

③' Based on the IEEE802.1X authentication MIB information collected in advance from the authentication switches, IncidentGuard identifies the port of the switch to which the search target host is connected and sets it as the candidate for the search result. It then retrieves the IEEE802.1X authentication MIB from the above switch and if the MIB shows that the search target host is still connected, it judges whether or not the port is the correct search result.

3.2 Automation of Search/Shutdown Operations

Previously, IncidentGuard relied on the manual operations of the operator for performing the search and shutdown operations. The current upgrade has made it possible to perform these operations by an automated processing method that is triggered by the reception of security event from the security devices, provided that the rules of operation are set in advance.

By setting the rules for the critical events that present a high potential for virus infection among the events sent from the security devices, this upgrade makes it possible to prevent the spread of virus infections without operator intervention.

4. Improvements Resulting from the Present Upgrade

The present development has made it possible to provide double cyber attack countermeasures. The IEEE802.1X authentication switch prevents unauthorized access at the time of connection and then IncidentGuard prevents virus infection spreading by isolating the infected client PC from the network even when a client PC is virus-infected due to a file being attached in a mail received during operation. This solution not only helps avoid virus infections due to PCs brought in from outside but also solves the problem of virus infections spreading during operation after the connection has been authorized. A diagram that explains unauthorized access prevention at the time of connection and the process of virus spreading prevention during operation is shown in **Fig. 3**.

In the case of ordinary network configurations, it is rare that switches which support the discovery protocol are placed at the edge of the network and the client PCs are usually connected through non-intelligent hubs. As a result, it has often been necessary to shut down several client PCs connected to a port, even when it is required only to shut down a single switch port. As the current upgrade has solved this problem by enabling the search and shutdown of authentication switches installed at the edge of the network, it is now possible to shut down the virus-infected PCs specifically, with pinpoint accuracy.

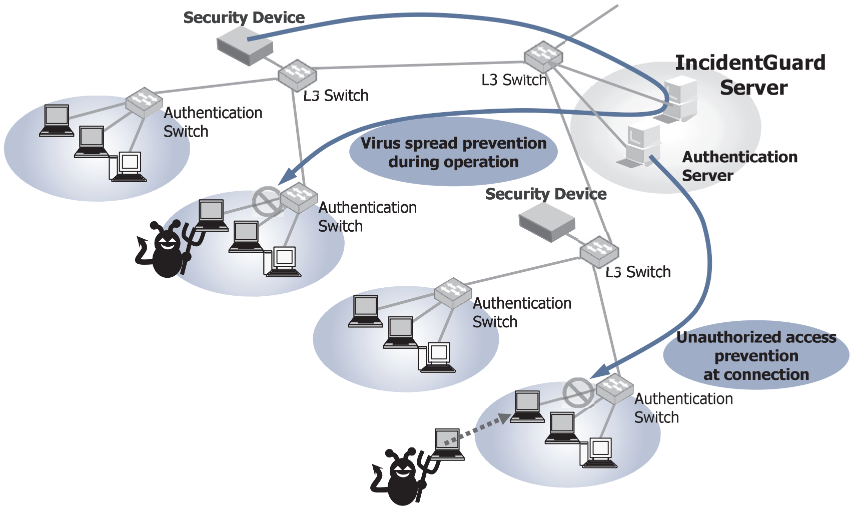

Fig. 3 A diagram explaining Unauthorized Access Prevention at the time of connection and prevention of virus spreading during operation.

When the shutdown of client PCs at the edge of the network is made possible by centralized control from the management software installed in the center in this way, it is no longer necessary to install network protection devices such as IDPs on a per-segment basis, so the cost of cyber attack countermeasures may thus be reduced.

5. Conclusion

In the above we outline “Cyber attack countermeasures based on WebSAM IncidentGuard and authentication switches” and describe the improvements that are effected by it.

For the present, this solution can be applied to the prevention of virus spreading in wired LAN environments. However, we are also examining the possibility of its application for the prevention of virus spreading in wireless LAN environments and will continue other studies to make the product compatible with a wider range of user requirements.

Since the need for the prevention of unauthorized access and virus spreading are increasing more than ever, we are determined to continue to provide security solutions that are suitable for easy introduction in many user environments.

Authors' Profiles

EBATA Kazumasa
Assistant Manager, 1st Computers Software Division,
Computers Software Operations Unit,
NEC Corporation

WATANABE Youko
Staff, Network Software Division,
Platform Operations Unit,
NEC System Technologies, Ltd.

NEZU Yuichirou
Staff, Platform Systems Division,
NEC Soft, Ltd.

TANIMURA Satoru
Staff, 1st Computers Software Division,
Computers Software Operations Unit,
NEC Corporation