Embedded Login Firewall

Intelligent Device Access Protection

Table of contents

1 Introduction

As IP video devices have become more connected and exposed to global networks, so too has their exposure to the threat from cyber-attacks. Attacks can range from simple attempted log-in using a dictionary attack to more sophisticated attacks such as cross-site scripting.

Since most cyber-attacks are based on unauthorized access and control of devices, our first line of defense is credential check and how log-in attempts are treated.

There are many methods in which credential checks can be implemented, and these can vary from vendor to vendor.

Many vendors simply increase the lock-out period with every wrong attempt. While this could provide a reasonable obstacle for an attacker it also has some drawbacks for clients with a wrong or incomplete configuration and for installers working to set up a system.
The disadvantage of this approach is that, if e.g. the user has a typo in his password he may be locked out for a few minutes before he can try again. In case this happens to an installer, it means valuable time and money for him and his customer.

Some vendors even lock out a user completely after a certain number of wrong attempts. For an installer, this means he has to factory default a device, not only dismissing the passwords but also all previous configuration settings that need to be done again.

We don’t want to lock out our own configuration tools and clients nor to place obstacles for our installers, so we implemented a more intelligent solution.

2 Embedded Login Firewall

The Embedded Login Firewall of all Bosch IP cameras, introduced with firmware version 6.30, consists of a two-level system which makes use of two integrated functional modules.

2.1 The logging module

The logging module observes clients’ log-in attempts and gathers information about these clients and their behavior:
- What server or service is targeted with the attempted log-in (RCP, HTTP, Terminal, Web service, iSCSI, FTP, SNMP)?
- Is at least one of the log-in credentials correct in the log-in attempt to any of these servers?
- Are there repeated log-in attempts and failures?

The module logs and memorizes up to the last 32 attempted log-ins to include client IP addresses, client actions and last access time.

2.2 The firewall module

The firewall module blocks access and data traffic from clients which are rated ‘suspicious’ by the logging module.
- TCP-Connections are blocked before they get connected.
- UDP Unicast and Broadcast packets are discarded before being processed by the application.

By blocking access and data traffic on socket level already, the Embedded Login Firewall requires only insignificant computational power to handle unauthorized access and is thus less prone to denial-of-service (DoS) attacks.

2.3 The decision tree

The intelligence in the Embedded Login Firewall is based on behavioral analysis. As long as there are 3 or fewer failed log-in attempts to a single server within 20 seconds, the system only observes.

For a human user, this period is typically too short to enter 4 wrong attempts triggering the firewall. Hence, the typical user will have the chance to continuously try to get his password correct without being blocked.

An automated system, like a configuration tool, e.g. Configuration Manager, or an attacking botnet, will try to get access to a device repeatedly and much faster.

If there are more than 3 failed attempts within 20 seconds, then the system choses between two modes:

► Blacklist mode

As long as all recently active clients can be stored in the history (32 IP addresses), the Embedded Login Firewall uses the “Blacklist” mode:

IP addresses which have never been successfully logged in and had more than 3 failed log-in attempts during the last 20 seconds are blocked.

This ensures that allowed clients are not blocked also while a fast attack is running.

► Whitelist mode

When the number of recently active clients exceeds the capacity of the history buffer, in other words, when the number of clients exceeds 32, the Embedded Login Firewall uses the “Whitelist” mode.

Then, only IP addresses, which were registered with at least one successful login to any server on the device within the last 24 hours are allowed to access. Access from a maximum of 32 clients which have been considered “good guys” is possible in this mode.

All other clients, most probably all the “bad guys”, are blocked until the number of failed log-in attempts drops below the alarm threshold of 3 wrong attempts within 20 seconds.

2.4 The benefits

The Embedded Login Firewall does not require any configuration. It automatically selects the appropriate level of protection to provide full transparency to positively acknowledged clients while blocking unauthorized log-in attempts.

The 20 seconds period is derived from user tests and balanced against probability. On one side, it is short enough that a human user would not experience any blocking while he tries to log in. On the other side, it is long enough to make any attack, and the results of it, unattractive to an attacker. Running a password hacking sequence would extend towards months, if not years, given the password being reasonably strong.

For Configuration Manager, a blocking due to misconfiguration of the password for device access would automatically disappear after 20 seconds once the password had been corrected. Same is valid for any other misconfigured client.

While the Embedded Login Firewall provides reliable access protection in case of an attack, it is quickly „self-healing“ once a password misconfiguration has been corrected, allowing all the “good guys” to seamlessly continue their work.

3 Glossary

TERM / ABBREVIATION	EXPLANATION
Client	A software component or tool that connects to a server or service on a host system by using specific interfaces and protocols
Credential	In IT context, credentials mean secret data that are required to identify, authenticate and/or authorize a user. The data could be e.g. passwords, keys, tokens, or certificates.
Cross-site scripting	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. Quoted from https://en.wikipedia.org/wiki/Cross-site_scripting
Cyber-attack	Any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. Quoted from https://en.wikipedia.org/wiki/Cyber-attack
Dictionary attack	In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. Quoted from https://en.wikipedia.org/wiki/Dictionary_attack
Firmware	Software, that is persistently installed and provides all functionality of an embedded device.
Human user	A person that behaves, thinks, acts and reacts, using tools to achieve something within its physical environment.
User	A person or automated instance, typically assigned with a user name or other identification data, which uses credentials to gain access to a system. A client may process those credentials for authenticating a user with a server or host system.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com
© Bosch Sicherheitssysteme GmbH, 2016

Author: **Konrad Simon, Product Manager IP Video**