Security Considerations for *Digital Signage*

White paper 1.0
by *SpinetiX*

08.2021

Scope of this Document

This white paper outlines the main considerations technical personnel should be aware of when determining the security risks and requirements for a digital signage project. We recommend that you take this document as a basis when auditing digital signage solutions against your IT security needs. This document is part of a series of our Digital Signage Security series.

Cybersecurity: Priority For Everyone

As our world becomes more digitized and interconnected every day, cybersecurity is more important than ever. The digital signage industry has historically largely ignored IT security best practices. Common sense says that as the prevalence of connected digital signage systems increases, the number of attacks will not diminish, so it is important to have security as a core requirement when planning, deploying and operating digital signage solutions.

When selecting products for a new project the security aspect, more often than not, gives way to other decision points such as acquisition price, operational costs, features, and performance. In addition, when planning and deploying a digital signage installation, you might have stakeholders with vastly different concerns towards security - typically, marketing and IT. This further risks security not being taken seriously into account.

New risks are emerging continuously, like the new "Ransomware as a Service" (RaaS) model which made headlines in 2021 with the REvil group and global infrastructure attacks on Kaseya and others and its new "double extorsion" tactics which seeks to monetize the threat of publicly disclosing stolen confidential information. It is therefore crucial that the security of a product be evaluated not only at time of purchase but also against the support policies and the availability of vulnerability patches during the lifetime of the product.

The Hidden Cost of Security

It is not uncommon to find digital signage players directly connected to the internet with no password or a default password. Most signage players run on unpatched and out-of-support operating systems with well-known vulnerabilities that can give attackers full remote access using off-the-shelf exploit kits. Yet performing regular updates is often regarded as a costly and unnecessary process that is better avoided and security is seldom a criterion when selecting a signage solution.

The hidden cost of unsafe hardware and software is however increasing fast. There are well documented cases of various network appliances being targeted to build huge botnets rented-out for a profit: Persirai (120’000 systems compromised) and Mirai (600’000 systems).

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)


***       gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

To quote a Trend Micro analysis: “in several high-profile and potent DDoS attacks, Linux-targeting Mirai revealed just how broken the Internet of Things ecosystem is. The malware is now making headlines again, thanks to a new Windows Trojan that drastically increases its distribution capabilities”.

In recent years there have also been countless other lower profile attacks specific to digital signage infrastructure, but no less damaging. The effects of these range from the relatively benign “please secure your system” message to ransom and even to display of hardcore porn in public places, like Washington’s Union’s Station.

Security is a
core requirement.

Why Security Matters

Decision takers often incorrectly consider all solution providers as equally secure and that the chances someone exploiting a vulnerability is negligible, or that the impact of a security breach is zero, none of which can be further away from the truth in the real world.

The risk of a security attack is real and not without consequences. A breach may cost you downtime, lost advertising revenue, and even your company image. A compromised digital signage installation can also be used to attack other IT infrastructure.

A common misconception is that a piece of software can remain secure without any action. Any software will have unknown, so-called “zero-day” vulnerabilities, so it is important that when they become known they are fixed in a timely manner and the fixes can be deployed efficiently.

Another common misconception is that signage players won’t be targeted by hackers. Actually, for a hacker any appliance is potentially a target if left unprotected because it can be used to gain further access to higher value targets inside the company network. Sophisticated attacks always try to find the weakest point of entry and internet-of-things appliances are a target of choice. This technique, called “Lateral Movement”, has become in 2019 one of the most important threats to enterprise networks by widely extending the list of entry-points for successful ransomware or data leak operations beyond those which are typically more heavily protected. Even as automatic updates have become more common, the Sunburst hack exposed in 2020 the reality of supply-chain attacks.

There are of course direct costs associated to security failures in the elements of a digital signage solution.

Compromised players have to be taken offline and are costly to restore. Compromised players or user accounts can be used to display reputation-damaging or illegal content. They can cause immediate revenue loss from advertisement or service contracts. If used as a conduit for a ransomware or sensitive personal information attack the level of damage can be devastating.

In addition, recent regulatory changes such as GDPR in the EU have made it important to select solutions that simplify compliance and reduce its cost.

Security Checklist

What you should consider when evaluating the security of a digital signage installation

In a digital signage network, there are numerous points where weaknesses are to be considered. The most visible one and easy to evaluate is the physical security at the screen location if in a public or sensitive place. Much more difficult to assess is the security of the digital signage player, the security of the display itself if connected and how protected is the network in which the player is installed.

Then there is the security of the content acquisition, distribution and production that also needs to be evaluated. And finally, how to ensure operators follow good security practices.

All these points should be considered from the start when selecting products and planning for digital signage. Adding security as an afterthought can be impossible or very costly once you are tied to a product.

Evaluating the security of a system is a hard problem, but there are a few basic questions that can ensure that the selected products follow good security practices. Use the checklist below to help assess your existing network and processes when choosing your future digital signage solution.

ON THE PROVIDER'S' SIDE:

The answers to the below points will indicate if you can depend on the manufacturer to properly maintain its product from a security standpoint.

□ Is the solution provider well established? Do they have a good track record?

□ Do they provide regular security updates on a timely schedule?

□ For how long will the selected product be maintained?

□ Do they have a working process for disclosing vulnerabilities, for example with the CVE list?

□ Do they have a well-defined release process including release notes with a list of security issues fixed in the update?

□ How are updates distributed and how costly is it to deploy these?

□ How good is the backwards-compatibility of updates? Does it have a good support service which you can reach?

ON THE SOLUTION'S SIDE:

Use the points below to help assess your existing network and processes or to when choosing your future digital signage solution.

- □ The content on screen is the one that was scheduled.
  - □ Avoid diffusion of malicious, illegal, or malevolent content by intruders or insiders and the ensuing damage to the reputation of the service provider.
  - □ Avoid revenue loss if sold advertising is not shown when and where agreed.
  - □ Availability and resilience targets ensure timely distribution of up-to-date content.
- □ The media player should not be a threat to the security of other equipment on the network: does not provide a weak point of attack that could be exploited for the theft of data or the dissemination of malware, spyware, or ransomware.
- □ Protects customer data on the player or cloud from being exposed to unauthorized 3rd parties. In case a security or data violation event happens, provides tools for forensic investigation.
- □ Integrates seamlessly with the customer's own IT security policies to protect its host network by supporting enterprise-grade protocols.
- □ Facilitates compliance with regulatory obligations, for example implementation of the GDPR directive in the EU or CCPA/CPRA in the USA.

The price of security.

All of this comes at a cost, and it should be no surprise that a secure solution is costlier, although the converse is of course not true. Developing secure systems is hard and thus has an extra cost. Maintaining a platform secure and actively monitoring vulnerability disclosures is time consuming and thus has an extra cost as well.

Once you have selected a provider that suits your security needs you should also apply sound security principles to the deployment and operation. Diminish the attack surface as much as possible by disabling unneeded services and do not expose the services on the network beyond what is really required for operations. Do not expose your devices directly on the Internet and use a firewall to protect the player's network. Ensure that operators are properly trained to not fall victim to social engineering attacks and use strong and unique passwords.

The bottom line.

All of this may seem like a lot to consider, but if the right security related questions are considered from the start of a project and the security aspects are integrated in the selection process it should not be that hard to choose the proper products that will diminish the risk of falling victim to a successful attack.

A Few Words **About the Authors**

Jean-Claude Michelou,
Vice President Research & Development

At SpinetiX Jean-Claude brings along his experience in the development of large scale, networked software infrastructures and complex technology project management. He is leading the company's development effort to build groundbreaking products.

After graduating from the Ecole Polytechnique in Paris (X94), Jean-Claude has held numerous research and engineering positions in Silicon Valley startups such as AltaVista and BigVine. He then co-founded VisioWave where, as vice president for R&D and chief software architect, he developed the video streaming technology that secures hundreds of public transportation systems worldwide.

Diego Santa Cruz, PhD
Technology Architect at SpinetiX

Diego has been passionate about SpinetiX product security for more than 10 years now, making every effort to deliver, secure, reliable and well-integrated products. He co-founded SpinetiX and is in charge of systems level development at the company.

Diego's main expertise covers systems and kernel development, network protocols, security, IT and electronics, as well as image and video systems, where he obtained his PhD. Author of several patents and an early Linux adopter, Diego was a contributor to the JPEG and MPEG committees.

SPINETIX™
N°1 IN DIGITAL SIGNAGE SOLUTIONS

Making your first steps in digital signage?

Looking for advice on security?

Contact us:

sales@spinetix.com

Read more publications from our Security Series:

spinetix.com/security

The trademarks and logos of other companies used here are to communicate that SpinetiX products and solutions integrate with these companies specified products and solutions. For the exact details of these integrations please contact SpinetiX. Unless expressly specified for a particular company, SpinetiX disclaims any other association, affiliation, sponsorship, endorsement or approval by these companies of SpinetiX or SpinetiX's products or solutions.