SECURITY IN DIGITAL SIGNAGE TECHNOLOGY

Toronto, March 2008

Background

Digital Signage, or Digital out-of-Home ("DooH") technology is becoming ubiquitous. The old way of communicating with customers out of their home environment, using paper posters sent around the country, is no longer very useful: these posters are static; they do not always arrive; they are costly to send; they are hard and costly to change; they are environmentally unfriendly, and they offer limited flexibility in terms of "narrowcasting".

This is where Digital Signage comes to the rescue. You can now send whatever media you like to whatever player groups. You can change the content whenever you like. The content can be moving, not static, and can be full-screen or use a split screen layout, or you can switch between the two at will. You can even add interactivity and RSS-based data feeds and weather forecasts.

Illustration 1: Digital Signage in practice

Just as important: you know when your players and screens work and when they do not. You even get proof of play "affidavits".

All this flexibility, however, needs to be very carefully implemented. If you can change content at will, can a clever hacker not do the same? Will all your stores be showing political or pornographic messages or skulls tomorrow? It has happened on more than one occasion and the consequences can be onerous to say the least.

When implementing DooH software, you need to be very aware of the need for security to avoid this. Risk is not acceptable in your DooH network, and experimentation is unwarranted.

The good news: establishing a secure network is not difficult if done right.

Security as a prerequisite

"Done right" means that security must not be built in as an afterthought. That cannot work. Rather, security in DooH software can be achieved by a careful risk assessment before writing the software, and an architecture that covers those risks, combined with the right policies and practices when actually running the network.

So how does that security work? First, a number of things are necessary from an architectural point of view. Those security prerequisites are:

- First and foremost, a secure architecture should connect *out*, not *in*. Meaning your signage players cannot be reached by inbound signals – neither yours nor the potential hackers'. This also means you have only one potential hack site to watch: the server. And watching one site is easier than watching hundreds or thousands.
- Your players should be behind a "NAT" (Network Address Translation") firewall that only allows outbound connections to be established.

- Additionally, your player itself should have a firewall enabled. This extra layer of "just in case" security is exactly the sort of things that delivers *real* safety.
- Be careful if players use DNS to find control servers: DNS can be compromised through a so-called "man in the middle"-attack. Using IP addresses makes it harder to transparently move data centre location, but is safer.
- You should use standard, robust protocols like FTP and HTTP for data transfer.
- Your control protocol should be transparent, so that you can ensure that your players do nothing untoward.
- As an extra security measure, you can consider using a VPN for your traffic.
- Web-based systems are preferred. You do not need to worry about security issues on local PCs affecting your network.
- You should only operate a web-based system using a secure ("HTTPS") connection; you should require secure password access to the system.
- You should allow access per defined user only to those functions that this user needs.
- Physical installation should be safe from interference. In particular, hide CD/DVD drive access and power buttons and cover IR ("remote control") ports.
- It should not be possible to simply push content into the player by inserting a CD/DVD or memory stick. Some kind of playlist mechanism, a security key structure, or a combination should prevent this.

Operational Security

In operation, too, you should keep certain security needs in mind.

- Use normal IT precautions. Are you actually patching your servers with software updates for security issues daily or weekly? Do not rely on "security through obscurity".
- Monitor your servers, and have warning systems in place in case of attack. Attacks are unfortunately very common on the Internet. Hiding is not a good idea.
- Change passwords regularly.
- Have players report on their health, and run regular network-wide player reports to spot anomalies.
- If you grant some "local access" to your system, ensure that local changes are approved and do not bypass your regular workflow.
- And importantly: check your play affidavits carefully for anomalies (e.g. files not being played enough; unknown files playing). That way if the worst should happen, you will catch the issue quickly, before much harm is done.

Time has shown that safe, reliable and above all secure implementations are very possible. If you follow the above advice, you can obtain the maximum possible safety through a combination of wise choices, good preparation, and a very small investment in time.

The author, Michael Willems, is Chief Technology Officer of EnQii (www.enqii.com), a leading international provider of Digital Signage Software and solutions.