

# Appliance Security

---

*Security Considerations For Implementing Computing Appliances*

by Kurt Keller (Kurt@pinboard.com)

last compiled 28<sup>th</sup> March 2005

## History

25<sup>th</sup> March 2005 initial version  
28<sup>th</sup> March 2005 minor adaptations

## Appliance Definition

In recent years the use of so called *appliances* in computing has increased. An appliance, sometimes also referred to as a *blackbox*, usually is considered to be a piece of hardware performing one specific function and doing so out of the box, with no or only minimal configuration. Such devices do have numerous advantages:

- No or only minimal setup required.
- No or only minimal backup required.
- No knowledge of the inner workings required.
- Plug-and-play replacement in case of failure.
- No underlying operating system to setup, configure and maintain.

Examples of appliances are, among others, certain types of virus scanners, encryption boxes, VPN concentrators, file storage devices, etc.

## Appliance Internals

When considering the internals of an appliance, most of the time it turns out to be nothing but another computer, tuned for one specific task. Just like a general purpose computer, it consists of an operating system and some application software. The operating system, be it a system for embedded devices or a typical general purpose system, usually can be configured for various tasks and with various services running. Generally the operating system will not only be tuned for best performance for the provided service, but also have all services, which are not strictly required, turned off. This stripping down of services is done for performance reasons on one hand and for security reasons on the other hand. In the same way, a well configured appliance will usually not run any applications except for the ones strictly required for the task at hand.

In most cases, an appliance could equally well be built from off the shelf hardware components

bought at the computer shop round the next corner. Performance might not be optimal, but generally it should be no problem. The same holds true for the operating system. Often an equivalent service could be built on various commonly available operating systems or even on a general purpose workstation.

## Threats

While vendors of appliances are interested in staying in business and thus will generally do their utmost in securing the systems they sell, mistakes and oversights are possible. Also included components, such as libraries etc. can suddenly turn out to be vulnerable.

In addition to these unintentional threats, which usually are considered, there also exists the possibility of intentional threats. Even though unlikely, it would be possible for an attacker, at least for some time, to build and market an appliance which secretly will help to attack the customer's network and data.

## Data Screening

One possible attack vector is data screening. For example, an appliance scanning all email for viruses does automatically have access to all email messages and, theoretically, would be able to secretly also scan all email for confidential information. Such information could then be sent back to the attacker periodically, be it by email, by a proprietary protocol masked as being used for daily virus pattern updates, or even by saving it to internal storage and have the machine intentionally fail after a certain amount of time, so it must be sent back to the attacker for repair or replacement.

## Passive Sniffing

Often appliances are directly connected to a customer's internal network, not sealed off from other machines by firewalls with very strict rules etc. In such an environment it might be possible, in addition to the advertised function, to have a passive network sniffer installed and running, trying to collect useful information. This information could then be passed back to the attacker.

## Trojan Horses

Many appliances need some connection to the internet for updating themselves; application or configuration data, such as virus patterns, spam patterns etc. Commonly the data flowing through such connections is not controlled by the customer, often controlling this data is not even possible as proprietary protocols are used. Such uncontrolled or uncontrollable connections could, for example, be designed so they can additionally be used for remote control of the appliance. This is remotely controlling a machine which usually is placed in the internal network of the customer. Even if no realtime remote control is implemented, automatic update procedures still could download jobs to run certain commands and pass the results back with the next scheduled update.

Another Trojan horse like attack would, for example, be possible with antivirus appliances. While performing good antiviral services the appliance itself or the antivirus pattern files could have code implemented to let specially signed viruses by the attacker slip through.

## Active Attack

An active attack by the appliance probably is the most unlikely method, as it can be assumed that it would be detected before long. However, if the customer does not have any access at all to the base system of the appliance and the attack is only timely limited, it might still be thinkable and, depending on how it is implemented, difficult to prove.

## Level of Trust

Most corporations ultimately trust their appliances. Not only for performing the advertised service, but also security wise. The appliance is purchased, configured with an IP address and other relevant parameters and connected to the network, all without much further thought about possible security threats posed by the appliance.

In many environments there exist strict rules on how to setup and harden a computer system and often such systems are also scanned for possible vulnerabilities regularly or at least before connecting them to the production network. Ordinary computer systems are not fully trusted.

Many companies require external consultants hired for installing machines to sign various agreements. Often the consultants are not allowed to bring in any removable storage media, are supervised and the machines they setup are checked carefully. While being trusted for their skills, external consultants often are not trusted equally in a security sense.

Security people usually are opposed to giving outside specialists remote access to internal machines, be it for debugging, remote administration or installation. Outside sites are untrusted.

Even though an appliance without system level access is a machine you know least about and thus theoretically is the most insecure computing device you can possibly have in your network, it is usually trusted most.

## Recommendations

Considering that an appliance basically is nothing but another, specialized, computer system, it should not be trusted more than any other computer system. In fact, an appliance should be viewed as a machine setup by an external consultant you do not know and who has not signed anything, in an environment you do not know or control, from sources you do not know and in a way you do not know and have no control over.

The rules for security screening should be at least as strict as for other machines connected to the network. Many appliances do not even allow the customer access at the operating system level, so checking what is going on ‘behind the scenes’ is especially difficult, if possible at all. Best security practices would mandate to

- Physically separate appliances from the rest of the network.
- Logically separate applications as much as possible from the rest of the network.
- Include appliances in your usual and regular security scans.
- Very strictly control what communication channels are open to and from the appliance.

- If possible control and verify the data going in to the appliance and coming out of it.
- If possible delete any permanent storage in the appliance before returning it for maintenance or replacement.

## Acknowledgements

This paper has been produced without much specific research into appliances. In its initial form, it is mainly representing the thoughts and knowledge of the author at the time of writing. Highlighting some issues the author thinks usually are not accounted for adequately when deploying appliances.