

## Xsdot Security system

The big benefit of using web applications and web sites is that they are easily accessible for anyone by using the internet. However, this also gives the drawback that the web applications are easily accessible to web site hackers, crackers and abusers. Therefore when applying web applications on a private network or public internet, a multi layer security system is of utmost importance to protect your data, users, customers, relations, web applications, hardware and software.

Xsdot implemented many security layers into its application and hosting platform to protect it's services from any damage. The combination of using these layers is also called 'Defense in Depth'.



### Defense in depth security platform

Defense in depth is the key factor to stop most network and computer-related attacks. With 'defense in depth' applied attackers usually become frustrated and move on or stop the attacks altogether. Our security platform can be divided in the following four main security groups.

#### Network and server protection

The first security layers are used to protect your network and servers (hardware and host software), this is accomplished by using a hardware firewall in front of the internal network and a software HIPS running at the server. The firewall protects on a network level while the HIPS protects on a server level. Xsdot partnered with Cisco™ and CA to get the best protection available.

The hardware firewall implements the following defense layers

- \* Authentication layer (IPSec, SSH, HTTPS, HTTP)
- \* Perimeter Layer (traffic filtering, network perimeter attack protection, denial-of-service attacks, session hijacking, unauthorized perimeter device access)
- \* Network Intrusion Prevention (grant access only to desired users, enforces rules specifying what those users can do and provided protection for perimeter attacks)

The host based intrusion detection and prevention system (HIPS) is the last defense layer and is installed on the hosts (servers). This layer protects the host and its software for the remaining traffic/requests that has passed the hardware firewall. The following protection applies,

- \* Protocol protection (HTTP, POP3, SMTP, etc).
- \* The host's operating system (Linux, Windows, etc)
- \* The host's software serving the internet (and other) services (web, mail, etc.) against buffer overflows, viruses, proxies, Trojans, etc.).

The HIPS contains thousands of attack signatures that are updated automatically for the protection against Zero-day attacks.

### **Web application authentication system**

Xsdot implemented a 3 layer authentication system into its web application server. By using authentication services, it is possible to give access or deny access to users on web servers, web application domains and specific web services and pages. As our web application server is hierarchical based our security system is also hierarchical based, easily apply authentication on web tree nodes.

Authentication is for example used to make private data and applications accessible to its belonging users, after authentication the users can access specific parts of data and services online.

### **Data storage and transportation protection**

To protect the data from third parties, the data is encrypted with three encryption methods/layers when stored plus one extra layer during the transportation. Furthermore our web applications are secured by SSL (secure socket layer) keys. Xsdot uses several reliable Certificate Authorities (CA's) for obtaining different types of SSL keys to secure its sites and applications.

### **Web services anti abuse system**

A huge issue for web applications is the constantly increasing 'web application abuse'. Web application abuse is typically performed by misusing interactive services like dynamic forms, forums, blogs, mail page modules, mailing registration systems, login systems, etc; basically any service that contains input characteristics is 'abuse-able'. Most abuse is 'just annoying', but some types can be very serious as well.

The abuse is commonly performed by hacked/infected home and personal computers, without the owners knowing this is happening (the real 'abusers' basically stay out of reach). Most abuse is performed for sending or posting spam, filling databases with spam or for redirecting internet users to spam or scam.

The xsdot anti-abuse framework contains 18 unique filters and functions to identify and block abusers. The framework works on a global per server basis and on a per service level (different services implement different abuse filter algorithms depending on the service nature).

### **Security & authentication components**

[User component](#)

[Group component](#)

[User group component](#)

User settings component

Logon indicator / Quick logon

Who is online service

Web services anti abuse system

Item security properties