SOLOVATSOFT
OFFSHORE PROGRAMMING

Security Programming Overview

❖ Experience in Security Applications Creation

SolovatSoft has over 15 years of developing Security Applications in Europe and the US. Some of the development projects and security highlights that we have done include:

1. Implementation of a secure data exchange protocol using Russian encryption systems for Military Defense Department.
2. In Russia our developers have patents for methods to provide special security features for database development.
3. Implemented the system architecture and programming methods to protect database (user management, audit, monitoring requests execution) and received Russian security certificate for system protection equal to B3 class.
4. Used algorithms DES, T-DES, AES and Russian cryptography algorithms in network drivers (direct and using OpenSSL libraries) in a variety of development programs.
5. Have worked as a dedicated team of 20 engineers for the last few years for a US company that develops security and policy management applications: we have developed two major security applications for this company. "Machine Audit" and "Management tool and Policy Creation tool" . We have worked for several years with another security solutions company to develop the security applications Enterprise Auditor and Patch Manager .

This is a short description of the "Machine Audit" and "Management tool and Policy Creation tool" applications.

❖ Policy creation tool

This Application monitors and tracks all traffic for an entire distributed network (many domains and many thousands of users) . The program monitors all communications by all users within the system:

- Destination;
- Application used for connection;
- Transport type;
- Port service and duration;
- Other source information including but not limited to Netstat:
    - All resources running on the desktop;
    - Mac;
    - IP;
    - OS;
    - Gather the authentication type and or location the user is getting his or credentials from example: Active directory, Radius, TACAC Plus, ACE

All processes are conducted in the Kernel space for speed and accuracy. No user space operations need occur.

A propagation option is implemented by means of the agent so that administrators do not need to push the agent to every desktop.

not require all the traffic to pass through it.

The system provides the ability to sort collected information by user, IP, domain, MAC address destination, port service, application, authentication type, authorization type, user name, etc.

The system allows taking the data discovered and builds it into a LDIF, Radius, and ACL access control policy. The key with this system is that the information collected is used to build policy, authentication, authorization or access control, for a domain, single computer and for a firewall at an edge. The general idea was not to limit the system to a particular type of policy but make it open enough to be extended with additional policy, data and information to be collected. The goal of the application is to be unobtrusive and non interruptive but gather information about the network and then render that information in policy for all levels of the network.

Technologies used:

- IDS systems to gather and watch all activity in a network;
- Audit gathering tools for the track packet information about the network;
- IPS for inspection of network operation;
- Packet inspection tools to watch all packet information;
- Network discovery tools;
- Network monitoring tools;
- Packet sniffing tools;
- Packet interception tools.

Machine Audit and Management tool

This application is designed to automate the stocking and inventory of computer hardware, software and other equipment in businesses. It keeps managers up to date on all computer and software in the company, tracks all changes in company's equipment, track computer and device movement inside the company and provides a wide range of reports to help in planning maintenance and renewing of company equipment and software. Most important it tracks security issues of the local network computers, manages resource access list, upgrades potential security risk computers, tracks and manage policy settings of the local network computers.

The major feature of the application is its capacity to provide immediate and up to date information about the company's computers, Software Park, manage and track policy and security issues of the local network computers from all locations (using its web interface) and provides cost saving by keeping all computers in sync.

The application provides solution which helps to automate software, hardware and equipment inventory process with the capability of storing a profile of all computers and their environment and maintenance history in a data base. Automatic inventory control protects computers and hardware from being stolen or displaced, protects the company from using stolen /not licensed software, protects the company computers and valuable information by providing detailed information about security issues found on every machine, protects the company computers by installing security critical updates on the system, saves detailed information about computer configuration in database and allows generating detailed reports on computer configuration. Scheduled inventory and reports generation allows scheduling computer inventory and reports generation tasks to be automatically generated when they are necessary in order to keep them up to date with all the changes.

Features:

- Automatic computer's hardware inventory;
- Automatic computer's software inventory;
- Automatic computer's policy inventory;

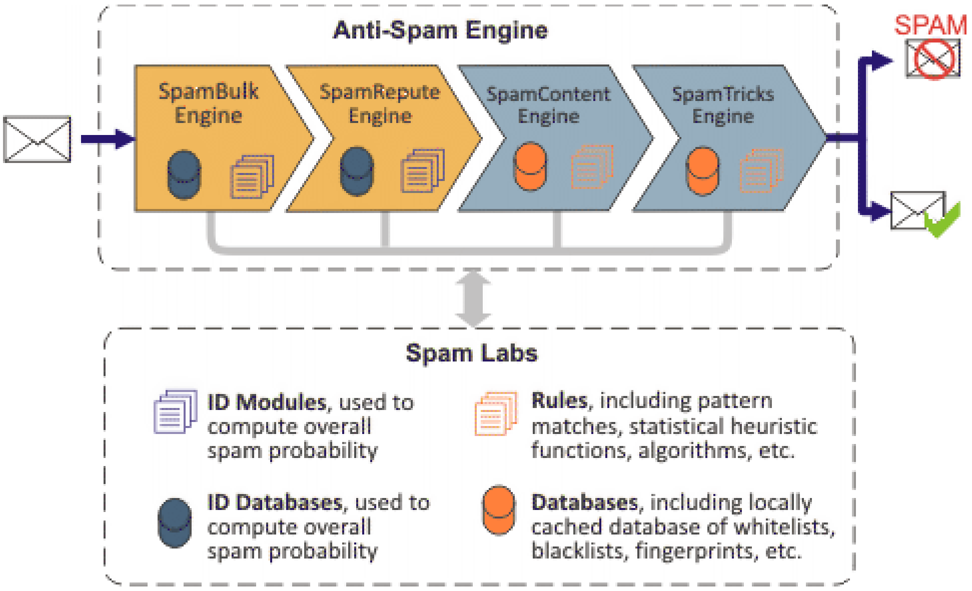
- Automatic computer's environment inventory;
- Keeps information about every hardware device available in company;
- Keeps information about hardware configuration of every workstation of the company;
- Keeps information about all software used in the company;
- Keeps information about all software installed on a single workstation;
- Real time monitoring of computer environment;
- Keeps complete information about hardware (serial numbers, manufacturer codes, manufacture date, date when a device was bought, date a device has been removed or replaced and so on);
- Scheduled reports generation;
- Scheduled computer inventory;
- Scheduled software inventory;
- Remote access to stored information from Internet and mobile devices;
- Customizable interface;
- Multi-user online access to database;
- Emailing reports;
- Support both MS SQL Server and MSDE for small companies;
- Grouping of computers for representation, reports generation and group operations purposes;
- Wide set of reports;
- Report exporting using user defined template;

Used API and technologies:

- WMI - Network Management
- Network Monitor
- Windows Security
    - CryptAPI
    - Authentication
    - Authorization
    - Management
    - Task Scheduler
    - Systems Management Server
    - Windows File Protection
    - Policy and profiles
    - Group Policies
    - User policies
    - System Policies
- Windows Base Services
    - Windows API
    - Processes and Threads
    - Services
    - Synchronization
    - Windows System Information
    - Interposes Communication

❖ OEM Spam Filtering Engine

The goal was to develop a spam filtering engine that offered information actuality, up-to-date categorization, scalability, reliability, framework flexibility and extensibility. The client needed an ability to scan as many URLs for as many categories/fraudulent practices/phishing/spam/viruses/etc. as possible.


Anti-Spam Engine
SpamBulk Engine
SpamRepute Engine
SpamContent Engine
SpamTricks Engine
SPAM
Spam Labs
ID Modules, used to compute overall spam probability
Rules, including pattern matches, statistical heuristic functions, algorithms, etc.
ID Databases, used to compute overall spam probability
Databases, including locally cached database of whitelists, blacklists, fingerprints, etc.

The project has been a two year and a fifteen developer effort which produced an OEM spam filtering engine with the following parts:

- SDK

  Anti-Spam SDK is a software library that provides classes to communicate with the spam filtering engine. Functions are provided to return a 'spam score' for each message.

  The SDK includes an API (Application Programming Interface) that allows developers to integrate Anti-Spam engine with other applications, along with more than 40 configuration options that allow OEMs to balance memory usage, throughput and detection.

- Image Spam

  The engine looks for image attributes that are unlikely to exist in legitimate email. These include, but are not limited to:

  - Jigsaw puzzle-style images.
  - CAPTCHA-style images that intentionally obscure content.
  - Images designed to emulate plain text.

  Though the presence of these techniques does not guarantee that the message is spam, scoring algorithms can penalize these messages to ensure consistently high accuracy.

  - Engine's image analysis is a subset of our approach to quantifying the reputation of each attribute of each message.
  - Engine treats images—and parts of images—as attributes that can be extracted and tracked over large numbers of messages.
  - Engine defines reputation of an attribute as the difference between the number of spam versus the number of legit messages for that attribute.

- Phishing

  The Engine combines its own home-grown reputation filters, along with global access to advanced data networks, to block phishing and other forms of email fraud.

  - Reputation analysis and email authentication help the system identify the rightful owners of IP addresses, domains, email address, and even message content.

- Engine’s global data network includes near real-time reporting of phishing outbreaks.

The SDK also includes an API to identify and segregate phishing from other types of spam. This allows OEMs to reject, delete, quarantine, etc., phishing attacks before they reach customers' inboxes.

Additional features

- ➢ Scan IP addresses for spam/legit attributes.
- ➢ Extensive Spyware Database
- ➢ Verify owner of an IP/Domain address and Software
- ➢ New Ximian Evolution plugin
- ➢ Ability to prevent, detect, and disinfect zombie machines
- ➢ Detection of viruses in real-time with and without signatures.
- ➢ New Novell Groupwise Plugin
- ➢ Custom override the weight of any rule.
- ➢ Block spammers who spoof domain names.
- ➢ Tune performance and accuracy by setting the size of the message to be read and to be scanned.
- ➢ Networks checks throughput can be increased by being used only when most needed.

Tools and Technologies

Supported platforms include: Linux (Certified for Redhat, Mandrake, and Suse), Microsoft Windows, Solaris 8 (Sparc), Solaris Intel, FreeBSD, AIX, Mac OS X, HP-UX

Languages and Tools: C/C++, Perl, PHP, Apache, Sendmail, Gcc compiler, Gdb debugger, Gprof, Valgrind memory leak checker, Flex text parser.

Contact Us

SolovatSoft

1300 S. El Camino, Suite 310, San Mateo, CA 94402

1-800-782-1746 Sales@solovatsoft.com

www.SolovatSoft.com