Technology Trend Report

Security in Next Generation Multimedia Networks

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
content filtering • traffic shaping • authentication

clavister™

Protecting Values

The telecommunications market is poised for fundamental changes. Security is a key business enabler and a necessity for the telecom providers that would like to stay in business today and in the future as well.

This paper provides an overview of the revolution of a locked-in industry that suddenly is brought to its feet, awakened by a multitude of commercial and technical threats that seemed to appear out of nowhere.

With a reasonable approach to security, however, the telecom industry has a lot to gain, new business areas to claim and profit from.

Clavister the leading provider of emerging security technologies and vendor of the world's first commercial UMA security gateway.

In this paper, Clavister describes the security needs in the next generation of multimedia networks and how the telecom industry can benefit from those needs.

Growth within mobile communications is enormous; in 2002 there were a billion mobile phone users and for the first time their number therefore exceeded fixed line telephone users. During 2006 the number of mobile users grew to over two and half billion with forecasts from iSuppli and others indicating that the four billion mark will already be broken by 2010.

New types of mobile telephones are reaching the consumer at a pace which has never been higher; the need to have access to all conceivable and inconceivable services seems nearly insatiable.

It could be thought that this ought to be a dream situation for established as well as dominant mobile operators such as Orange, Vodafone, T-Mobile, and Deutsche Telekom.

The telecommunication suppliers, who have the opportunity to deliver the network, equipment and expertise which makes the mobile world a reality for the user, ought to be in the same pleasant situation. Companies like Ericsson, Siemens, Alcatel and Nokia have grown to multi-national giants who have long dominated the industry and should therefore be well equipped for the fantastic growth being experienced.

However there are clouds in the sky which make the situation not as perfect as it at first seems.

The telecommunications industry has traditionally been a closed world where access to and understanding of mobile technology was limited to the engineers who have grown up within the walls of an Ericsson and who have been central in establishing telecommunication standards and solutions.

To establish, build up and manage large scale networks for mobile communications, because of this closed world, has been the domain of just a few companies able to make the large investment in technology that has been necessary. These companies have often been state owned and, as part of later privatization, have been remolded into the telecom giants found in today's market. Naturally there are cases where private newcomers have also succeeded in taking up positions in the mobile arena.

This traditionally closed telecommunications world is now exposed to a new challenge from an area long considered separate, namely the Internet. In parallel with mobile growth, the expansion of the Internet and Internet based services has occurred at record speed, and in most households and businesses in the industrialized world Internet access is not just a fact, in many cases it is a necessity for access to a society's important services.

In contrast to the closed mobile communications industry, the Internet is a textbook example of openness and cooperation. New standards and technologies are spread to anyone interested; while researchers and engineers work together across company boundaries to find solutions which best take development forward.

In the beginning, the telecommunications industry said in a relaxed way; how can this apparently nearly hobby-like and anarchic enterprise harm the billions worth of investments made in GSM and 3G networks?

Today however, the industry takes the Internet seriously. Openness and general accessibility to standards and tools on the Internet have led to the development of services and communication possibilities which weren't thought possible before. Anyone with Internet access can now make use of IP-telephony, video-on-demand. chat and other services at extremely low cost; in some cases for free.

A telling example is Skype which makes telephony possible over the Internet without any costs except an Internet subscription. Skype began as a project as late as 2003, and already has today many millions of users.

In order to counter the choice and the possibilities that the Internet offers, the mobile industry was subject to enormous pricing pressures. From 1993 to 2006 revenue per call minute has fallen from $70 US dollars to around 15 cents. The amount of calls has certainly increased along with new subscribers, but operator profitability has been pressured all the more.

The telecommunication industry needs in other words, to find new ways to create profitability and to keep, as well as take back, those customers who would otherwise use the alternative solutions that the Internet offers.

Fixed-Mobile Convergence (FMC) and the New Multimedia Network

It is clear that mobile telephony alone no longer yields the revenue base needed for the large mobile operators. A line of other services therefore needs to be able to be offered to consumers and companies and in as cost-effective and user-friendly way as possible.

Messaging services such as SMS and MMS were among the first services which complimented pure mobile telephony, but currently niche-services, video-calls and mobile TV are a reality and going strongly forward.

In telecommunications there is talk of a repositioning towards multimedia and networks for multimedia services. This is seen most clearly in the reorganization which Ericsson underwent at the end of 2006, where a new business division was created just for multimedia. Ericsson's many recent acquisitions within this area sends the same signal; the industry is changing from delivering telephone calls to offering complete solutions for multimedia services, where traditional telephony is just a part.

At the same time as these multimedia services have been and continue to be created at an ever faster pace, the possibilities for accessing these services have increased. In the telecommunication world these are known as *access technologies*.

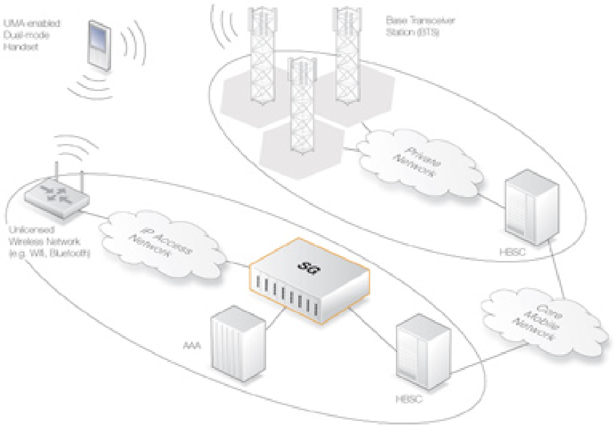
The most widely distributed access technology is of course radio based GSM (with additions such as GPRS for access to certain additional services). In certain areas a technology called Wimax is also delivered which can be viewed simply as radio-based broadband.

For laptop users another access technology has become very popular, namely WiFi, with which public places such as airports, hotels etc. are able to nearly always offer wireless connection for it's customers.

Combine with this the broad rollout of different broadband connections to households and companies, and it is easy to realize that the variety of access technologies alongside the radio network represents a significant threat to the established mobile operators.

In order to retake control in the telecommunications world, a trend has been developed in the industry which is called Fixed-Mobile Convergence (FMC). In summary, FMC is a philosophy where all services will be accessible from all types of equipment, independently of access technologies.

A concrete example of this development is a new type of solution for mobile telephony which is called UMA, Unlicensed Mobile Access. Simply described, UMA means a call from a mobile telephone can be sent not only over traditional GSM radio but also over so-called WiFi hotspots which are situated in the home and connected to the mobile operator's network via the Internet. The picture below illustrates the UMA solution.



With UMA, mobile operators have two major advantages; the first is to reduce the level of usage of the already overloaded radio network, which reduces the need for expensive investment in new radio network. The second is that subscribers are inclined to use the mobile telephone more often even in the home, which is totally in keeping with the philosophy behind FMC, and at the same time take income from the fixed telephone network.

The Need for Security in the New Multimedia Network

Underlying the telecommunication industry's investment in FMC and multimedia is the acceptance of the standards and technologies that dominate the Internet which is further evidence for the breakthrough power that the Internet has.

With the case of UMA cited above as an example, the household's broadband connection is used to transport telephone calls over the public Internet.

This adaptation to Internet standards is naturally positive from a general perspective, but at the same time creates a whole new challenge for operators in the form of the problems of offering the services in a secure way.

As long as mobile services were suitable for a radio based network using difficult to obtain technology, the security risk wasn't particularly high. It required both access to expensive radio equipment as well as deep technical knowledge to be able to misuse the mobile network, which meant that vulnerability was, in reality, very low. The move to open and Internet based standards has on the other hand, meant that, by and large, anyone can gain access to simple tools and methods which can be used to doubtful ends and thereby cause large financial as well brand related damage to operators.

To illustrate the need for security, UMA can again be used as a case study.

As mentioned earlier, the public Internet is used in a UMA scenario to carry telephone calls between the mobile telephone and the operator's network, usually called the "mobile core" network, which comprise the operator-owned network which provide all the equipment and functions needed for mobile services to function.

The way the Internet is built means that mobile calls will be transported over a variety of networks and equipment which the operator doesn't own and even less controls. This means in practice that unauthorized persons can listen in to calls, which naturally is totally unacceptable from an integrity viewpoint.

Another consequence is that unauthorized and anonymous users on the Internet can easily pose as paying subscribers and thereby make use of operator's services for free, or even worse, use other subscriber's identity to commit illegal acts.

It is of course an imperative for operators to shield themselves and their subscribers from these security threats, Even if UMA is used, as in an example above, the same problem applies for all types of new access technologies and networks with which multimedia services are launched.

In other words there is a very powerful financial motivation and incentive for why security is today a highly prioritized issue for the telecommunications industry.

The need for High Performance Security Products

The changes that are now taking place in telecommunications towards a multimedia driven network with a large choice of multimedia services also entails a much greater need for high capacity, so-called bandwidth, in the network.

An ordinary telephone call doesn't require particularly much bandwidth, whereas services such as video-calls, online games and so on, require significantly higher capacity. Offering video-on-demand services with HDTV quality places enormous requirements on transfer speed.

To understand the dimensions, a telephone call can be said to require 128 kilobits per second of broadband whereas an HDTV film requires upwards of 16 megabits per second; that is to say, a difference 120 times greater.

Besides modern services requiring significantly greater capacity in the operator's network, there is also a rapid increase in the capacity of both company networks and home networks. Most company networks are today based on, or migrating to a so-called gigabit-network with as much as ten times higher performance than that which was usual just a few years ago. Concurrently, a standardization of technologies is taking place which allows a further 100 times more capacity.

Earlier security products have been seen as somewhat unusual and less important components and therefore have had a relatively low profile in the network. As the need for security has escalated, exactly for the reasons described earlier, so have security products now taken on a different status and are counted as being amongst the most important building blocks in the modern telecommunications network.

This means of course that the security products installed in the modern telecommunications network can not be allowed to create capacity bottlenecks. On the contrary, security products are required whose performance can grow at the same pace that the network grows and new services are launched.

Security as a Source of Income

In the description above, security and security products are put forward as a pure cost, albeit a necessary one, in being able to offer secure services. Correctly applied though, the need for security can be used by operators to create entirely new revenue streams.

Just a few years ago, security was relatively straightforward and simple for most companies to manage; if there was a virus problem then an investment was made in an antivirus product. If there was a need to filter traffic then an investment was made in a firewall and so on.

Today security is a long way from being so easy to manage; the amounts of attacks grow continuously while at the same time the attacker and the threat is becoming all the more complex and have greater negative effects on business operations.

In order to counter the threat, new security technologies are being continuously developed which means that today's security products are enormously complex in comparison with earlier ones. Today's IT administrator who manages and maintains security equipment therefore needs to have broad expertise and be able to manage everything from traditional firewall technology to intrusion detection, antivirus, content filtering, user control, peer-to-peer protocols, instant messaging and so on. The list of security technologies grows almost exponentially.

All this means that the IT administrator, who is, as never before, already overloaded with user support and the management of the enterprise's systems, no longer has the opportunity to perform an active security role.

These problems have laid the foundations for an entirely new type of business where the supplier with high expertise in the security field offers complete management and maintenance services for the enterprise's security infrastructure. This type of supplier is often referred to as a Managed Security Service Provider, MSSP.

A typical scenario is that the MSSP installs security products in the customer's network and then manages and maintains these products from a central location.

The big disadvantage with this type of MSSP solution is that it demands physical products installed in each individual customer's network environment, which involves both investment and more expensive costs if the products require hardware maintenance or replacement.

Here the operators who move towards FMC have an excellent opportunity to offer MSSP services in a significantly more cost effective way than that described above. Because the operators own or have direct control over the access network, the security products can be moved away from the customers and into the operator's own network. This naturally yields advantages of scale for the operators; centralized solutions involve fewer products to maintain and administer, and also a lower investment threshold.

With respect to products, a centralized MSSP solution has identical demands to those described above. Performance is of course of the highest importance where individual products must be able to manage the capacity needs of many customers. A technology called virtualization is also critical in a well-functioning MSSP solution. virtualization technology means that a physical security product can be segmented into a number of logical or virtual units where each virtual unit is managed and is perceived as a self-contained, single product.

How Clavister Can Help

For over ten years, Clavister has been developing products and solutions for network security. For a number of years, Clavister has been highly active in research and development work where security within the new telecom networks is the focus. As an example the results from this work is the fact that Clavister produced and shipped the world's first commercial security gateway for UMA/GAN networks.

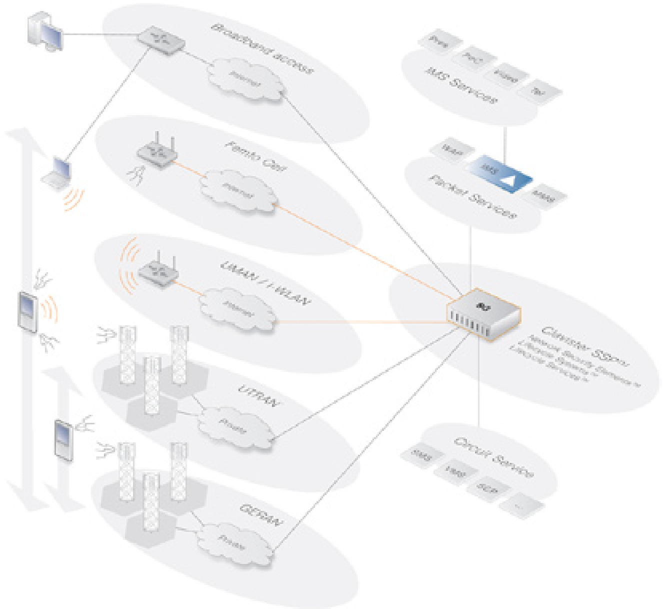
Clavister can today offer a concept named Clavister SSP™, Security Services Platform. Clavister SSP™ is a modern technology platform consisting of a number of products and components that enables an operator to deploy and maintain security in modern telecom networks. In addition, Clavister SSP™ provides the opportunity to offer security as a value and revenue adding managed service. In short, Clavister SSP™ is the only tool needed for turning a big potential problem into secured business and new business potential.

Clavister Security Service Platform

Clavister SSP™ is a collection of products and services for the complete operation of network security.

At the heart of Clavister SSP™ is Clavister CorePlus™, a purpose-built network security operating system that provides a multitude of network security features, ranging from denial-of-service attack protection through various virtual private networking protocols and user authentication mechanisms, to advanced deep inspection capabilities with streaming anti-virus and intrusion prevention features. With over thirteen major releases over the years, Clavister CorePlus™ is clearly the one of the most mature security software on the market today.

Clavister CorePlus™ is available in a range of complete turn-key products, ranging from the powerful Clavister Security Gateway 5500 Series, for example being used as the tunnel terminating gateway in multi-access networks, down to the small Clavister Security Gateway 10 Series which is primarily used as customer-premises equipment.



Example of where the Clavister Security Gateway 5500 is used as a tunnel terminating gateway in an multi-access environment."

Clavister CorePlus™ is also offered on a pure software licensing basis for partners that would like to incorporate security functionality into their own systems, for instance using modern Advanced TCA platforms and alike.

In addition, Clavister SSP™ includes a set of operation and maintenance (O&M) tools that assist security administrators with anything within the management lifecycle. Clavister FineTune™, for instance, is a complete element management tool with full centralized management capabilities. Clavister PinPoint™ provides graphics-rich visual dashboards with key-performance indicators for all security aspects and a visual designer that allows administrators to build their own dashboards for their network operation centers. Clavister Insight™ is a modern security information and event management system with support for hundreds of device types and thousands of various reports.

Finally, Clavister SSP™ includes a rich palette of services made available by Clavister's highly skilled Professional Services division. A qualified team of field application engineers, technical support engineers and product trainers are available to make sure that the deployment of security is seamless and error-free.

Find out more about Clavister and Clavister SSP™ on www.clavister.com.

About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnsköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at www.clavister.com.

Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Clavister SSP™ Security Services Platform
firewall • VPN termination • intrusion prevention • anti-virus
content filtering • traffic shaping • authentication

Protecting Values