Case, Dowty-Case, Cray, Case Technology Legacy Products
Case Communications
NEWSLETTER
Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below.
[Subscribe/Unsubscribe]

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/Enquiry]**

Welcome,

Welcome to the Case Communications Newsletter . This month we look at Internet Telephony identity fraud, Mobile data units for 27 Police Forces, take a look at IP Sec, and more problems with the NHS IT project.

Identity fraud hits net telephony

A new type of identity fraud, which sees hackers tapping into voice-over IP telephony accounts, has been highlighted by a VoIP equipment maker.

[More]

Staying safe and taking risks

Should we have two internets asks Bill Thompson

[More]

Skills continue to command higher salaries for IT workers than certifications do, but some specific networking certifications have bucked the trend.

In its 30th quarterly IT pay index, Foote Partners found that specialties such as networking security and wireless networking certifications attract premium salaries, but - overall -- IT shops are looking for more well-rounded networking pros.
[More]

---

27 Police Forces to be given mobile data devices

Police across the UK will receive mobile data devices to be used on the beat as part of a £50m investment from the government.

The funding was announced by policing minister, Tony McNulty, and will see around 10,000 handheld computers distributed to 27 police forces across the UK.

[More]

Technical Overview - Security P Sec

Case Communications developement engineer Cal Leeming takes a brief look at IP sec.
[More]

NHS Fires Fujitsui from National Programme for IT

The £12.7bn National Programme for IT (NPfIT) was hit by another setback yesterday as one of the three key suppliers to the project was fired.
[More]

Mobile phone sales in Western Europe decrease 16.4%

Mobile phone sales in western Europe decreased 16.4 per cent to 35.9 million units in the first quarter of 2008, compared with the same period last year.
[More]

Case, Dowty-Case, Cray, Case Technology Legacy Products
Case Communications
NEWSLETTER
Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Identity fraud hits net telephony

Usernames and passwords from voice-over IP (VoIP) phone accounts are selling online for more than stolen credit cards, Newport Networks has found. The information allows someone to use the telephone service for free. Net telephony fraud is still in its infancy, with eavesdropping on calls being the most common security flaw.

Capturing accounts

But the move into stealing usernames and passwords which are routinely sent across the network when a call is made, is a worrying new trend thinks Dave Gladwin, vice president of products at Newport Networks.

"It is still at an embryonic stage but as voice adoption increases it becomes more of a problem and needs addressing," said Mr Gladwin.

The details are not sent as plain text but are encoded in such a way as to be "easily captured and unobscured", said Mr Gladwin.

Credit card details have been traded fairly openly online for some time and can be bought for around $12 (£6) each. VoIP account details fetch a slightly higher price, at $17 (£9), according to Mr Gladwin.

The problem is less of a issue for businesses which routinely offer voice-over IP services for their employees because users are tied into a secure corporate network.

But for consumers, relying on public or unsecured home wi-fi networks, there is more of an issue.

"90% of carriers don't offer a secure VoIP service," said Mr Gladwin.

He estimated it would cost around £2 / £3 per subscriber for service providers to instigate the additional level of security needed.

"Most of the software out there has the capability of running in secure mode if the service providers would accept it," he said.

VoIP provider Skpe said its service, unlike some of its rivals, offered end to end encryption.

"It doesn't matter whether I'm on an open wireless connection, there is no way someone could get hold of my username or password," said Jonathan Christensen, general manager of audio and video at Skype.

He accepts there are security issues facing the industry, especially for providers that use "less robust security mechanisms" but he questions how big a draw a free VoIP account would be for net criminals.

This is a view shared by Jupiter analyst Ian Fogg.

"I have not seen security issues with VoIP as a big issue. This is partly because such services aren't that mainstream and therefore have not been targeted by criminals in the way that e-mail and online banking services have," he said.

Story from BBC News

Case, Dowty-Case, Cray, Case Technology Legacy Products
Case Communications
NEWSLETTER
Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Staying safe and taking risks

Jonathan Zittrain's recent book, The Future of the Internet - And How to Stop It, has spurred a lot of discussion both online and offline, with blog posts lauding his insights or criticising his over-apocalyptic imagination.

The book itself makes fascinating reading for those who have watched the network grow from its roots in the research community into today's global channel for communications, commerce and cultural expression.

And the distinction that Zittrain makes between computers and devices that are open for hacking, exploration and creative use and those which are locked down and limited is one that we can clearly see.

An iPhone and an Asus Eee PC are very different objects, and I can't imagine anyone scrawling 'this machine kills fascists' on their iPhone in homage to Woody Guthrie, while my son has just done this to his Asus.

Red and green
“Perhaps we should …….. offer two separate networks, operating over the same physical connection”, says Bill Thompson.

One of the reasons that Zittrain puts forward for the growing popularity of closed or, as he prefers 'tethered', devices, is that they are less vulnerable to hacking, security flaws, malware and all the other perils that face any internet-enabled system.

But he sees great dangers in allowing the creative potential of our computers to be limited by the need to register programs with companies like Apple, or have Microsoft's approval before your software will run on Windows.

And because he's from the United States, he doesn't believe that the government or a regulatory framework can solve the problem.

Instead he calls on the internet-using community to come together to solve the serious problems that face us, and offers his own suggestions as to where some of that effort might go.

One of his more interesting suggestions is that our PCs and laptops should have two operating modes: red and green. In the green zone the system is locked down, only approved programs can run, only demonstrably safe traffic is sent and received, and safety is as assured as it can be.

The red zone is more like today's network, where you can download and run pretty much any software you like, but you run the risk that the movie file you found on BitTorrent is actually carrying a nasty little virus.

Users could then decide whether they want to work in the safe zone or go out onto the wider network. And, crucially, the red zone would have a 'restore' button that would wipe anything bad and return you to its initial state so you could recover from any infection.

It's a nice idea, and I think a lot of home users would choose a safer, if more limited, online experience.

Space for subversion

But unlike Zittrain I think that regulation can help, and that putting control in the hands of democratically elected governments is far better than putting it in the hands of corporations.

He wants the network's users to solve the problems, but a community on its own is far less effective than one backed by the rule of law, as eBay clearly demonstrates.

It can only operate as it does because contract law and financial regulation provide a way for the community to enforce its decisions against members, and this is true for other online services.

However not all governments are good; not all governments are wise and sensible; and not all governments listen to reason.

It is therefore necessary to ensure that, whatever the architectures of control on tomorrow's network, there is space for subversion, for activism, for stuff that is not approved, not countenanced by the state, not strictly legal.

And even if we accept that trusted systems will define the online experience for most people, most of the time - and that they will accept and even benefit from that - there needs to be more.

Perhaps we should extend Zittrain's idea beyond the computer and onto the network itself, and offer two separate logical networks, operating over the same physical connections.

One would be the safe world of electronic toll roads, the other a collection of dark and dangerous back alleys.

We could have a special virtual operating system for the uncontrolled internet, and anyone who wanted to use it would simply have to run it.

Of course things are not yet as bad as Zittrain seems to claim, and though I don't often agree with noted free market advocate and libertarian Adam Thierer, his critical review on the Progress and Freedom Foundation blog is well-argued and often insightful.

Safe place
As he notes, he can 'see no reason why we can't have the best of both worlds - a world full of plenty of tethered appliances, but also plenty of generativity and openness.'

But the desire to have a safe space online is growing stronger, and the pressure to lock down large swathes of the online world in order to make the network safe for the vulnerable will not go away.

We've seen it just this week with Facebook announcing that it will attempt to block access to its service to people convicted of 'sex offences' in the US, even though many of them will be guilty of nothing more than consensual sexual activity with other adults in public places.

But because the effort of checking whether someone was convicted - and not merely cautioned - for an offence which involved children is too great tens of thousands of people will be blocked from accessing the service.

Perhaps having a place where no such unreasonable and arbitrary distinctions exist is a good reason to start working on an alternative network

Story from BBC News

It would not be hard to build such a system.
Many of us already use what is called 'virtualisation' technology to run different operating systems at the same time, like the Mac users who also have Windows on their computer.

Case Communications

Case, Dowty-Case, Cray, Case Technology Legacy Products

NEWSLETTER

Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Skills continue to command higher salaries for IT workers than certifications do, but some specific networking certifications have bucked the trend.

David Foote, co-founder and CEO of the Vero Beach, Fla.-based firm, said the push for more outward-facing IT, which requires more soft skills and often less specialized technical prowess, was driving the change in hiring and salary practices.

Overall, the market value of IT skills the survey tracked increased 6% over last year, while the corresponding value of the 164 certifications tracked was down 3%.

"If you look at the certification market, it's oriented toward deep-dive technology," Foote said. "The trend is a much broader view of who an IT person is." Larger percentages of the IT budget are being dedicated to customer-facing initiatives, he said, requiring a broad range of talents for successful execution.

"Companies are looking for industry experience, customer experience … and not so much technical stuff," Foote said. It's a trend that has hurt those first entering the field, where a few certifications are no longer enough to guarantee a position. Experience is now mandatory, he said, but it can be demonstrated in a number of ways, from summer jobs to showing work experience from a related field.

Despite the call for generalist IT professionals, Foote said, there are still several niche, "new IT" skills that command a premium, particularly in the networking field.

"If you look at growth, virtualization has been fantastic for networking people," Foote said. Certifications and experience in storage, network security, wireless network management, RFID, and IP telephony are hot right now, he said, and these are the cutting-edge fields where the deep-dive approach is still very much needed.

Network security management and wireless network management both saw market value growth between 20% and 25% over the six months preceding April 2008.

"With the exception of the wireless stuff, a lot of it is inward, technical work," Foote said.

The overall trend in IT, including networking jobs, favors the adaptable and flexible, he said, even if that means sacrificing more specialized knowledge.

"The skills market has expanded over the years outside of certification," Foote said. "Skills … have been on the rise."

Case, Dowty-Case, Cray, Case Technology Legacy Products
Case
Communications
NEWSLETTER
Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

27 Police Forces to be given mobile data devices

The aim is to increase the time police officers can spend on the beat by cutting down on paper work and reducing the need to return to the police station to file reports.

The project is a collaboration of the Association of Chief Police Officers the Association of Police Authorities and the National Policing Improvement Agency (NPIA).

Richard Earland, NPIA CIO explained that officers will be able to access databases such as the Police National Computer and command and control systems.

McNulty said the move was one of a number of improvements to "cut unnecessary bureaucracy, exploit new technologies and enable police officers to spend more time on front line policing".

The Met Police in London is one of the 27 forces to be getting the devices along with the British Transport Police, all eight Scottish forces and all three in the Yorkshire region.

Forces applied for a share of the funding to the NPIA, detailing training and plans in place to have the necessary infrastructure ready by September 2008 or March 2009.

Case, Dowty-Case, Cray, Case Technology Legacy Products
Case Communications
NEWSLETTER
Specialists in high-speed and rugged access solutions
Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Technical Overview - Security P Sec

Introduction

IPsec protocols operate at the Network Layer layer 3 of the OSI Model. Other Internet security protocols in widespread use, such as SSL, TLS and SSH , operate from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting layer 4 protocols, including both TCP and UDP , the most commonly used transport layer protocols. IPsec has an advantage over SSL and other methods that operate at higher layers: an application doesn't need to be designed to use IPsec, whereas the ability to use SSL or another higher-layer protocol must be incorporated into the design of an application.

Security architecture

IPsec is implemented by a set of Cryptographic Protocols for (1) securing packet flows, (2) mutual authenticationand (3) establishing cryptographic parameters.

The IP security architecture uses the concept of a security association as the basis for building security functions into IP A security association is simply the bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Therefore, in normal bi-directional traffic, the flows are secured by a pair of security associations. The actual choice of encryption and authentication algorithms (from a defined list) is left to the IPsec administrator.

In order to decide what protection is to be provided for an outgoing packet, IPsec uses the Security Parameter Index (SPI), an index to the security association database (SADB), along with the destination address in a packet header, which together uniquely identify a security association for that packet. A similar procedure is performed for an incoming packet, where IPsec gathers decryption and verification keys from the security association database.

For multicast, a security association is provided for the group, and is duplicated across all authorized receivers of the group. There may be more than one security association for a group, using different SPIs, thereby allowing multiple levels and sets of security within a group. Indeed, each sender can have multiple security associations, allowing authentication, since a receiver can only know that someone knowing the keys sent the data. Note that the relevant standard does not describe how the association is chosen and duplicated across the group; it is assumed that a responsible party will have made the choice.

Current status as a standard

IPsec implementation is a mandatory part of IPv6 but is not an integral part of IPv4. However, because of the slow uptake of IPv6, IPsec is most commonly used to secure IPv4 traffic. IPsec protocols were originally defined by RFC's 1825 & 1829, published in 1995. In 1998, these documents were obsoleted by

RFC 2401, RFC 2412 which are not compatible with RFC 1825 & RFC 1829 , although they are conceptually identical. In December 2005, third-generation documents, RFC 4301 & RFC 4309 were produced. They are largely a superset of RFC 2401 & RFC 2412 but provide a 2nd Internet Key Exchange standard. These third-generation documents standardized the abbreviation of IPsec to uppercase “IP” and lowercase “sec”. It is unusual to see any product that offers support for RFCs 1825 & 1829. “ESP” generally refers to RFC 2406, while ESPbis refers to RFC 4304.

Design intent

IPsec was intended to provide either transport mode (end-to-end) security of packet traffic in which the end-point computers do the security processing, or tunnel mode (portal-to-portal) communications security in which security of packet traffic is provided to several machines (even to whole LANs by a single node

IPsec can be used to create Virtual Private Networks (VPN) in either mode, and this is the dominant use. Note, however, that the security implications are quite different between the two operational modes.

End-to-end communication security on an Internet-wide scale has been slower to develop than many had expected. Part of the reason is that no universal, or universally trusted, Public Key Infrastructure (PKI) has emerged (DNSSEC was originally envisioned for this); another part is that many users understand neither their needs nor the available options well enough to promote inclusion in vendors' products.

Since the Internet Protocol does not inherently provide any security capabilities, IPsec was introduced to provide security services such as the following:

1. Encrypting traffic (so it cannot be read by parties other than those for whom it is intended)
2. Integrity validation (ensuring traffic has not been modified along its path)
3. Authenticating the peers (ensuring that traffic is from a trusted party)
4. Anti-replay (protecting against replay of the secure session).

There are two modes of **IPsec** operation: **transport mode** and **tunnel mode**.

Transport mode

In transport mode, only the payload (the data you transfer) of the IP packet is encrypted and/or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be translated as this will invalidate the hash value. The transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers). Transport mode is used for host-to-host communications.
A means to encapsulate IPsec messages for NAT Traversal has been defined by RFC documents describing the NAT-T mechanism.

Tunnel mode

In tunnel mode, the entire IP packet (data plus the message headers) is encrypted and/or authenticated. It must then be encapsulated into a new IP packet for routing to work. Tunnel mode is used for network-to-network communications (secure tunnels between routers, e.g. for VPN's) or host-to-network and host-to-host communications over the

Internet

Technical details
Two protocols have been developed to provide packet-level security for both IPv4 and IPv 6:

- The IP **Authentication Header** provides integrity and authentication and non-repudiation, if the appropriate choice of cryptographic algorithms is made.
- The IP **Encapsulating Security Payload** provides confidentiality, along with optional (but strongly recommended) authentication and integrity protection.

Cryptographic algorithms defined for use with IPsec include HMAC-SHA1 for integrity protection, and triple DES-CBC and AES -CBC for confidentiality. Refer to RFC 4305 for details.

Authentication header (AH)
The AH is intended to guarantee connectionless integrity and data origin authentication of IP datagrams. Further, it can optionally protect against replay attack by using the sliding window technique and discarding old packets. AH protects the IP payload and all header fields of an IP datagram except for mutable fields, i.e. those that might be altered in transit. In IPv4, mutable (and therefore unauthenticated) IP header fields include TOS, Flags, Fragment Offset. TTL and Header Checksum. AH operates directly on top of IP, using IP protocol number 51. An AH packet diagram:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

Field meanings:

Next header
Identifies the protocol of the transferred data.
Payload length
Size of AH packet.
RESERVED
Reserved for future use (all zero until then).
Security parameters index (SPI)
Identifies the security parameters, which, in combination with the IP address, then identify the security assocation implemented with this packet.
Sequence number
A monotically increasing number, used to prevent replay attacks.
Authentication data
Contains the integrity check value (ICV) necessary to authenticate the packet; it may contain padding.

Encapsulating Security Payload (ESP)
The ESP protocol provides origin authenticity, integrity, and confidentiality protection of a packet. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

Unlike AH, the IP packet header is not protected by ESP. (Although in tunnel mode ESP, protection is afforded to the whole inner IP packet, including the inner header; the outer header remains unprotected.) ESP operates directly on top of IP, using IP protocol number 50.

An ESP packet diagram:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
	Padding (0-255 bytes)		
		Pad Length	Next Header
Authentication Data (variable)			

Field meanings:

Security parameters index (SPI)
Identifies the security parameters in combination with IP address.
Sequence number
A monotonically increasing number, used to prevent replay attacks.
Payload data
The data to be transferred.
Padding
Used with some block ciphers to pad the data to the full length of a block.
Pad length
Size of padding in bytes.
Next header
Identifies the protocol of the transferred data.
Authentication data
Contains the data used to authenticate the packet.

Implementations

IPsec support is usually implemented in the Kernel with key management and ISAKMP / IKE negotiation carried out from user-space. Existing IPsec implementations tend to include both of these functionalities. However, as there is a standard interface for key management, it is possible to control one kernel IPsec stack using key management tools from a different implementation.

Because of this, there is confusion as to the origins of the IPsec implementation that is in the Linux Kernel. The Free Swan project made the first complete and Open Source implementation of IPsec for Linux . It consists of a kernel IPsec stack KLIPS as well as a key management daemon (Pluto) and many shell scripts . The FreeS/WAN project was disbanded in March 2004. OpenSwan and Strongswan are continuations of FreeS/WAN. The KAME Project also implemented complete IPsec support for NetBSD, FreeBSD . Its key management daemon is called racoon OpenBSD   made its own ISAKMP/IKE daemon, simply named isakmpd (which was also ported to other systems, including Linux)

However, none of these kernel IPsec stacks were integrated into the Linux kernel. Alexey Kuznetsov and David Miller wrote a kernel IPsec implementation from scratch for the Linux kernel around the end of 2002. This stack was subsequently released as part of Linux 2.6, and is referred to variously as "native" or

"NETKEY".

Therefore, contrary to popular belief, the Linux IPsec stack did not originate from the KAME project. As it supports the standard PF Key protocol (RFC 2367) (and the native XFRM interface for key management, the Linux IPsec stack can be used in conjunction with either *pluto* from Openswan / Strongswan *isakmpd* from OpenBSD project, *racoon* from the KAME project or without any ISAKMP/IKE daemon (using manual keying).

The new architectures of network processors, including multi-core processors with integrated encryption engines, change the way the IPsec stacks are designed. A dedicated Fast Path is used in order to offload the processing of the IPsec processing (SA, SP lookups, encryption, etc.). These Fast Path stacks must be co-integrated on dedicated cores with Linux or RTOS running on other cores. These OS are the control plane that runs ISAKMP/IKE of the Fast Path IPsec stack.

There are a number of implementations of **IPsec** and ISAKMP/ IKE protocols. These include:

- 6WINDGate Network processor MPU Fast Path IPsec stack
- NRL IPsec, one of the original sources of IPsec code
- OpenBSD with its own code derived from NRL IPsec
- the KAME stack, that is included in Mac OS X, NetBSD and Free BSD.
- "IPsec" in Cisco IOS Software
- "IPsec" in Microsoft Windows including Windows XP, Windows 2000, Windows 2003 and Windows Vista
- IPsec in Solaris
- IBM AIX Operating system
- IBM z / OS
- IPsec and IKE in HP-UX (HP-UX IPSec)
- "IPsec and IKE" in VX Works

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

NHS Fires Fujitsui from National Programme for IT

After 10 months of contract re-negotiation the NHS has fired Fujitsui from its National Programme for IT.

NHS Connecting for Health (CFH), which runs the NPfIT, insisted the move was in the best interests of the taxpayer.

"Regrettably and despite best efforts by all parties, it has not been possible to reach an agreement on the core Fujitsu contract that is acceptable to all parties," said a spokesman.

"NHS CFH has to continue to protect the interests of the taxpayer and preserve the basis of contracts which ensure payment on delivery."

The NHS CFH supplier contracts work on a strict "payment by delivery" basis.

It is understood that the NHS were demanding more flexibility in Fujitsu's services – Fujitsu wanted more money to provide this flexibility.

Fujitsu is the second major supplier to drop out of the programme after Accenture exited in 2006 citing profitability issues.

CFH says work has started immediately on planning the necessary arrangements to replace Fujitsu.

It is thought BT is the most likely candidate to take over the area as the patient record software being used in London – the area BT supplies – is the same as in the southern region that Fujitsu was supplying.

The other likely option is CSC

But CSC already runs two of the five areas of the Programme, and has also recently been selected as a preferred supplier for the ID cards programme.

And a switch to CSC would probably mean installing iSoft's Lorenzo Software in the Southern region, rather than the Cerner Millenium Software BT is familiar with.

Case, Dowty-Case, Cray, Case Technology Legacy Products

Case Communications

NEWSLETTER

Specialists in high-speed and rugged access solutions

Case Communications May Newsletter

Case Communications May Newsletter

In this Issue:

Archives

Read the back issues
Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter
If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts
If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Mobile phone sales in Western Europe decrease 16.4%

It was the first drop since 2001, when research group Gartner started tracking the market.

But worldwide sales reached 294.3m units, up 13.6 per cent on the first quarter of 2008.

Developed markets were the worst hit amid the economic uncertainty, said Carolina Milanesi, research director for mobile devices at Gartner.

“While sales in emerging markets continued to be driven by strong net new subscribers’ growth, mature markets felt the pressure of an uncertain economic environment,” she said.

“Sales of high-end devices in particular were lower as consumers turned to mid-tier devices when looking to upgrade their old phones."

"Phone manufacturers should strengthen their mid-tier offerings to cater to those users who might be reticent to invest too much money in replacing their old phone when the economic environment remains challenging.”

Nokia maintained its market lead, selling 115.2 million mobile phones in the first quarter of 2008. But to ward off increasing competition the company will have to improve usability and design and continue to integrate new technologies into its handsets, said Gartner.