

Converged Video Network Security

How service providers can counter the various security risks associated with implementing IP Video

IPTV can create new revenue sources or enhance existing ones, but proper security is required. These inherent security risks need to be addressed to help ensure successful business results.

This white paper:

- Describes the main threats by hackers and fraudsters to video deployment
- Discusses the three key technologies used to protect video application intellectual property rights
- Describes how to use the ITU X.805 framework to develop a comprehensive model to counter threats to a generic converged video infrastructure



Contents

Introduction	3
Threats to IP Video Deployments	3
Protecting Intellectual Property	4
Content Protection Systems (CPS)	4
Conditional Access Systems (CAS)	4
Digital Rights Management (DRM)	4
VOD and Broadcast	5
Countering the Threats	6
Threat References	8
Threat Models.....	8
Make Secure IP Video a Reality	14
Author	15

Introduction

Although IP Video has created new service and revenue opportunities for traditional voice and data carriers, the technology also comes with a high level of risk due to attacks by fraudsters and hackers. However, with the proper planning, development and implementation of effective security processes, this risk can be managed efficiently and cost-effectively.

Threats to IP Video Deployments

Compared to traditional voice/data networks or cable TV infrastructure, threats to an IP Video environment are far more severe. IP Video allows carriers to manage valuable content that must be protected from unauthorized access and modification. Carriers also need to ensure that quality of service is protected to comply with customer's expectations and Service Level Agreements (SLAs).

For years the satellite TV industry has been fighting access fraud¹. Recently, satellite TV companies have been taking legal action against defendants for unauthorized access to TV content.²

The experience of the satellite TV industry shows that fraudsters go to great lengths to break their security measures. This includes cracking the smart card protection used for the set top boxes and distributing cloned "free access" cards. Even though the satellite TV providers have modified the cards, fraudsters have managed to find alternative ways to break the safeguards incorporated in the new releases.

Now that video technology has entered the IP world, the level of threats has escalated – vulnerabilities that have been solved in other, more mature technologies are still part of the new IP Video systems.

IP Video is not only transferred to set top boxes, but also to computers, which facilitates hacker access. Simple software modifications introduced by hackers allow them to break the encryption system and other security measures, or even capture and redistribute the contents using peer-to-peer networks.

A major impact on the satellite TV industry has been fraudsters selling modified "all access" smart cards. As a result, the IP Video industry faces an entirely new threat – with broadcasting stations residing on every home PC, hackers are able to redistribute the broadcast stream to other computers all over the world.

¹ See http://www.theregister.co.uk/2004/12/11/directv_hacker_sentenced/

² See http://www.directv.com/DTVAPP/aboutus/headline.dsp?id=03_03_2005A

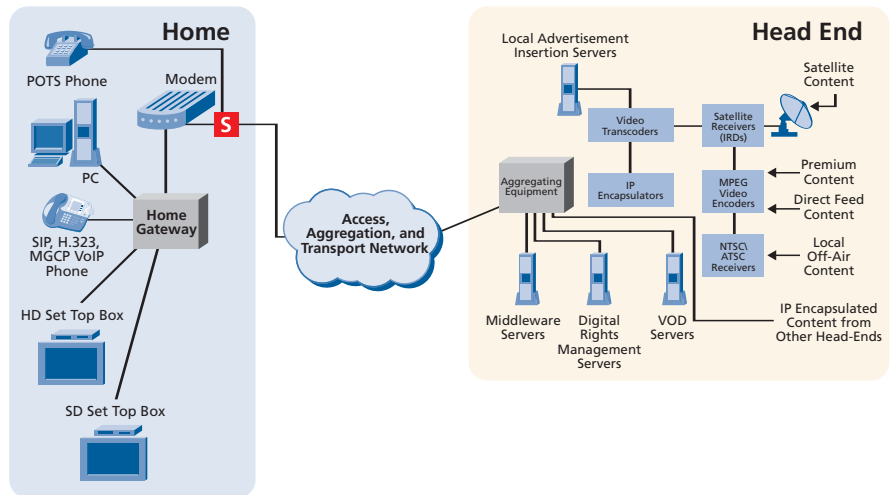


Figure 1. IPTV Network Architecture.

Protecting Intellectual Property

There are currently three primary types of technologies used to protect video application intellectual property (IP) rights: content protection systems; conditional access systems; and digital rights management.

Content Protection Systems (CPS)

Content is transmitted across networks in an encrypted form to help protect against theft or unauthorized access.

Content Protection Systems are used to help ensure that content is only viewed by authorized subscribers. Even if an intruder has access to the communication, content should be encrypted. Handling of key management process, including how keys are exchanged between parties and change frequency, is an important security issue.

Conditional Access Systems (CAS)

CAS helps ensure that only authorized subscribers have access to the content, creating a safeguard against theft of service.

These systems are used by cable operators to control access to content. CAS has evolved from simple frequency shifts and electronic noise to content encryption. Because telcos and carriers face different threats associated with IP video, a variety of new technologies have been developed to protect data.

Digital Rights Management (DRM)

Content owners realize that IP Video provides a great channel, but is also a huge risk. The growth of peer-to-peer networks demonstrates that digital content can easily be traded on the Internet with little content owner control and without proper recognition of IP.

DRM manages how the content is used by the subscriber based on specific conditions set by the distribution contract.

Technology providers initially implemented solutions that lacked strong DRM control. Today, despite current baseline DRM controls, some vendors are still failing to address the issue of recording and replay – subscribers can store copies of DRM material and redistribute it on the Web. This has prompted content owners to take matters into their own hands and begin implementing strong DRM controls to reduce the risk of unauthorized access to content.

VOD and Broadcast

There are currently two basic options for content delivery using IP Video: video on demand (VOD), and broadcast. Each has its own particular security and DRM requirements.

For VOD, it is generally recommended that the content be segmented and encrypted using a symmetric key. The key can be changed several times in a typical movie to increase protection. Each set top box has the subscriber's private key, and the VOD server sends the encrypted content and the encrypted symmetric keys to the set top box for decryption and playback.

Broadcast content follows a very similar process. Content is encrypted at the source with a symmetric key. The set top box sends a request for the current content key, and the content server sends an encrypted symmetric key to be used by the set top box to retrieve the contents.

Current industry trends indicate that content owners are demanding relatively strong encryption for their data, including the implementation of Advanced Encryption Standard (AES)³. This will probably shift attacks from content to the end points and the transport layer.

³ See <http://www.screenplays.bz/sp105o.html>

Other DRM requirements include the stipulation that DRM protected information should be unintelligible after leaving the source. It should only be decrypted after it has arrived at the destination. This involves changing the security architecture to include a Key Repository that is used as part of the encryption process.

Smart Cards and DRM

Although other technologies are also in use, smart cards are one of the most widely used technologies to facilitate the authentication process and protect video over IP. These cards contain an embedded microprocessor that can be used to store security information such as private keys for digital signatures. Without a smart card there is no second level authentication. This allows hackers to simulate the details from a valid subscriber and steal access to the service.

The satellite and cable TV industries have used smartcards for some time and, even with known cases of card fraud, recognize that the use of cards is one of the best ways to reduce the risks of unauthorized access and content fraud.

DRM systems are currently being integrated with smart cards and private key storage to enable the encryption of content from the source and allow the creation of specific streams for each subscriber. Smart cards are used to authenticate the subscriber, which allows service operators to encrypt packets and send the key to the subscriber's set top box.

The smart card also facilitates the process of using different encryption keys during the broadcast process, thus increasing the complexity and resources required to break the security of the content.

Even after the smart card encryption has been breached, fraudsters have the added problem of distributing the cloned cards. The logistics related to this process create a barrier and reduce the impact of access fraud. (Without the cards, fraudsters can simply distribute software modules that enable unauthorized access to the contents. A similar situation occurs with regard to the "Content Scramble System" (CSS) protection implemented for DVDs.⁴)

DRM has also been implemented on iTunes, and there are claims that a free piece of software⁵ can be used to access DRM protected files and create an unprotected version.

⁴ For example, Jon Johansen, a Norwegian, posted software on the Internet that allowed anyone to open the CCS protection and access the DVD's contents.

⁵ See <http://www.videolan.org/>

⁶ See <http://www.itu.int/home/index.html>

⁷ ITU X.805 Press Release : <http://www.lucent.com/press/0304/040317.bla.html>

"It is paramount that security be a well-thought process that goes from system inception and design to system implementation to policies and practices for system deployment," said Houlin Zhao, director of the Telecommunication Standardization Bureau for the ITU. "Lucent and Bell Labs understand security, and they recognize the importance of a standards-based approach for realizing it. I applaud their work in driving the development and adoption of Recommendation X.805 – a significant step on the path to securing networks worldwide."

Countering the Threats

A very effective way to analyze the threats to the infrastructure is to use the ITU X.805⁶⁷ framework to develop a comprehensive threat model for a generic converged video infrastructure.

Some of the threats to this type of network include:

- Denial of service attacks and worm propagation
- Network infrastructure attacks
- Trojan horse programs and customer's theft of service
- Self provisioning infrastructure attacks
- Billing infrastructure attacks
- Intellectual property (IP) theft

Lucent Bell Labs played an important role in the development of the ITU X.805. The ITU X.805 recommendation provides a framework for a thorough review of all aspects of security in an IP Video solution.

There are eight security dimensions that cut across the management, control and end-user security planes of the X.805 framework. Each plane has its own underlying infrastructure, services and applications. This encompasses everything from the IP backbone through the video application middleware, to the video head office and finally the set top box.

The eight dimensions are:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

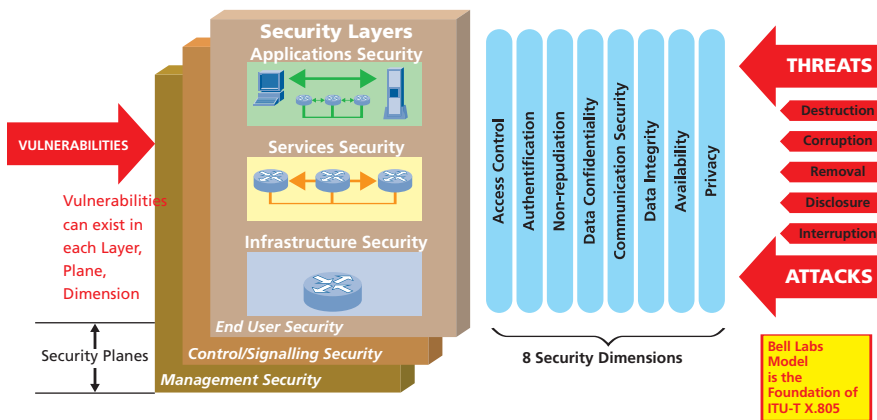


Figure 2. Applying security dimensions to security layers.

The intersection of each security layer with each security plane indicates where security dimensions are applied to counteract the threats.

Table 1 provides a mapping of security dimensions to security threats. The mapping is the same for each security perspective. The symbol ✓ in a cell formed by the intersection of the table's columns and rows indicates that a particular threat is countered by a corresponding security dimension.

Security Dimension	Security Threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	✓	✓	✓	✓	
Authentication			✓	✓	
Non-Repudiation	✓	✓	✓	✓	✓
Data Confidentiality			✓	✓	
Communication Security			✓	✓	
Data Integrity	✓	✓			
Availability	✓				✓
Privacy				✓	

Table 1. Mapping of security dimensions to security threats.

There are several threats to the IP Video service but in comparison with other broadcast technologies, the security implementation is relatively easy.

Some of the threats that should be included as part of an IP Video Risk Assessment include:

Threat References

When unscrupulous advertisers started sending unsolicited e-mail to thousands of email addresses it was called SPAM. Then Instant Message systems were targeted and that was termed SPIM (SPAM over IM). Voice over IP can also be a target for unsolicited calls and it too has its own name – SPIT (Spam over IP Telephony).

Now, IP Video technology needs to implement protections against SPIV (SPAM over IP Video). If set top boxes and applications are not configured to authenticate/validate sources of content, they will end up displaying unsolicited pop-up advertisements.

IP Video is supported by known operating systems and commercial networking equipment. In the case of viruses and worms, a disruption can be caused to the service either by saturation of the networks or by crashing the network elements. To prevent those incidents, normal patching and testing is required. Worms might crash supporting services such as billing or provisioning. If the incident happens during a particular VOD selling time, then the vendor will suffer a revenue loss.

As content becomes more valuable and entertainment systems began to integrate known operating systems, fraudsters will attempt to use Trojan horses to steal access to content. Subscribers might inadvertently install software that allows intruders to gain access to content and even request VOD using the subscriber's account. It is difficult to avoid this situation and it requires constant interaction with the system, automatic updates and anti-virus packages to maintain protection.

Intruders might try to control the provisioning infrastructure or the billing infrastructure as part of a fraud attempt either by creating "ghost" accounts or changing the entries in the billing system. If proper auditing and monitoring systems are not implemented, intruders might be able to change information from the central applications.

Threat Models

The following threat models describe the different layers and planes of a video IP infrastructure:

ITU-T X.805 Threat Model for Video IP

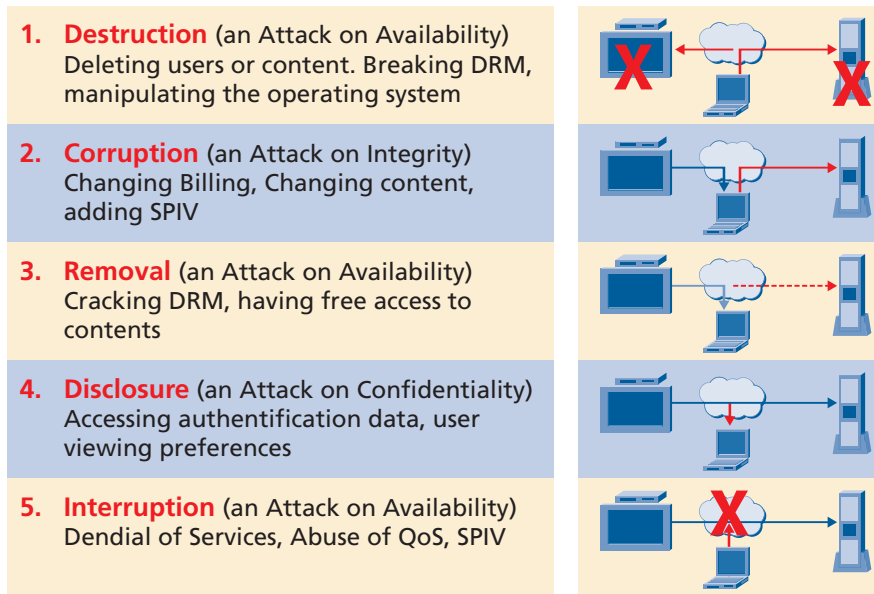


Figure 3. ITU-T X.805 Sample Threat Model for Video IP

Application Layer, Management Plane Threat Model

Securing the management plane of the application layer is accomplished by controlling the application management data.

As part of securing the management plane, the following controls should be implemented when securing the Application Layer, Management Plane:

- **Access Control** – Ensure that only authorized personnel are allowed to perform administrative activities on the application, such as administering video on demand requests and having access to content lists and descriptions.

Only authorized users must undertake the remote management of set top boxes, central office equipment, broadcast network equipment and different elements related to the broadcast head end. Intruders planning to manipulate the configuration of the different elements can use default parameters and vulnerable services. Lack of appropriate access controls could result in denial of service attacks, access fraud, and man in the middle attacks.

- **Authentication** – Verify the identity of the person or device attempting to perform network application administrative activities.

Hackers will target the applications in attempts to gain unauthorized access to content and data. Identities must be verified to minimize the risk of unauthorized access to content. Access control is linked with the authentication of users. The identity of all system users must be confirmed.

- **Non-repudiation** – Provide a record of all individuals performing administrative actions on network applications.

This control also helps reduce the incidence of subscriber fraud – for example, service provisioning to “ghost” accounts. Most system updates are carried out using automated tools –set top boxes and networking elements must require non-repudiation parameters from the management terminal. This type of transaction could involve digital signatures of configuration scripts, or it could involve the use of management terminals to establish a secure connection before sending the information.

- **Data Confidentiality** – Protect all files used in the creation and management of the application.

Controls to reduce the risks of information disclosure should be implemented in order to protect customer details and administrative information. All the customer information must be protected from third-party access including electronic records of customers and configuration information which should be encrypted to avoid unauthorized access.

- **Communication Security** – Ensure that the management information flows only between the application and an authorized party.

Because worms and hackers may attempt to send management information to different network elements, controls should be implemented to prevent third-parties from gaining access to management communications. Man in the middle attacks can potentially be prevented by protecting communications security. Intruders could attempt to capture information sent by the management terminal to the various network elements. Set top boxes send and receive configuration information that can be manipulated by intruders if not properly secured.

- **Data Integrity** – All configuration and management information and data from the application should be protected from unauthorized modification.

This prevents intruders from modifying the data and causing system failures.

- **Availability** – Ensure that the ability to administer the application is not affected or denied.

- **Privacy** – Ensure that information that can be used to identify network-based applications is not disclosed to unauthorized parties.

Application Layer, Control Plane Threat Model

Securing the control of signaling information supports securing the control plane of the application layer

The following controls should be implemented when securing the Application Layer, Control Plane:

- **Access Control** – Ensure that application control information received by a network device participating in a network application originates from an authorized source.

The different parameters received should be protected as third-parties can manipulate part of the control process. It is very important to implement access controls so only valid elements are used for particular services such as DHCP, DNS and others.

- **Authentication** – Verify the identity of the origination of application control information sent to network devices participating in the application.

- **Non-repudiation** – Provide a record identifying the person originating the application control information.

All control information should include non-repudiation data. This involves either digital signatures or log details of the system and account used to deliver the information.

- **Data Confidentiality** – Protect application control information resident in a network device being transported across the network.

Application data should be protected from third-party access, as intruders could try to capture control information, session keys and other data.

- **Communication Security** – Ensure that application control information being transported only flows between authorized nodes. This includes protection against man in the middle attacks.

Application Layer, End-User Plane Threat Model

Securing the end-user plane of the application layer includes securing user data provided to the network-based application.

The following controls should be implemented when securing the Application Layer, End-User Plane:

- **Access control** – Ensure that only authorized users are allowed to use the network application.

- **Authentication** – Verify the identity of the user attempting to use the application

- **Non-repudiation** – Provide a record identifying each user who accessed the application.

- **Data Confidentiality** – Protect end-user data that is being transported or stored by the network-based application.

- **Communication Security** – Ensure that end-user data is not diverted or captured by unauthorized third-parties.

- **Data Integrity** – Protect end-user data that is being transported by a network-based application against modification, deletion or replication.

- **Availability** – Ensure that access by authorized end-users to a network-based application is not denied.

- **Privacy** – Ensure that the network-based application does not disclose information about the end-user.

Services Layer, Management Plane Threat Model

Securing the management plane of the services layer includes securing the operation, administration, maintenance, and provisioning of network services.

The following controls should be implemented when securing the Service Layer, Management Plane:

- **Access Control** – Ensure that only authorized personnel and devices are authorized to perform network service management activities – for example, granting a user access to the service.
- **Authentication** – A person's identity should be verified before allowing them access to administrative functions on the service layer.
- **Non-repudiation** – A record should be kept of all individuals performing network services administrative tasks.
- **Data Confidentiality** – The network services management information should be protected from unauthorized access – this includes passwords, configuration and parameters.
- **Data Integrity** – Management information of network services should be protected against unauthorized modification, deletion or replication.
- **Availability** – Measures should be implemented to ensure the ability of administrators to manage the network services at all times.
- **Privacy** – Ensure that information that can identify the administrative management systems is not available to unauthorized personnel.

Services Layer, Control Plane Threat Model

Securing the control plane of the services layer includes securing the control of signaling information used by the network services.

The following controls should be implemented when securing the Services Layer, Control Plane:

- **Access control** – Ensure that all control information received by the different elements has been sent by an authorized source.
- **Authentication** – The identity of any element sending control information should be verified.
- **Non-repudiation** – A record should be kept identifying all elements sending control information.
- **Data Confidentiality** – All control information stored or sent across the network should be protected against unauthorized access.
- **Communication Security** – All service control information should flow only between the intended source and destination.
- **Data Integrity** – Service control information held in network devices or servers should be protected against unauthorized modification.

Infrastructure Layer, Management Plane Threat Model

Securing the management plane of the infrastructure layer includes securing the operations, administration, maintenance, and provisioning of the individual network. The configuration of an individual switch is a typical management plane activity.

The following controls should be implemented when addressing the security of the Infrastructure Layer, Management Plane:

- **Access Control** – Ensure that only authorized personnel or devices are allowed to perform administrative activities on the network devices or communications link. This control applies to all the various elements involved in the communication. Without proper access controls, intruders could modify the configuration of communication elements and cause service interruptions, steal service, or create a man in the middle attack.
- **Authentication** – Verify the identity of the person or device performing the management activities on the network elements. Proper authentication of devices helps reduce the impact of man in the middle attacks and ensures that downstream elements accept information only from authenticated elements. Worms tend to rely on unauthenticated communications to infect other elements.
- **Non-repudiation** – Maintain a record of all individuals or devices that undertake administrative activities on the network elements. Any change to the system must be matched against an individual or device. This improves auditing capabilities and facilitates any forensic investigation.
- **Data Confidentiality** – Protect network communications against unauthorized access or viewing. This involves all data related to the infrastructure layer, including configuration information, authentication data and backup data. If configuration information is sent without protection, intruders may be able to capture configuration and authentication information.
- **Communication Security** – Data flow should be protected for secure remote management and administration. Ensure that communications are not diverted or intercepted. This control is also important when protecting against man in the middle attacks.
- **Data Integrity** – Administrative and management information must be protected against modification to prevent intruders from modifying instructions and configuration data. Measures should be implemented to avoid changes to configuration data.
- **Availability** – The ability to manage the network devices or communications links should be protected. Information about the configuration of the different systems should be available at all times. High availability and distributed infrastructures should be implemented to reduce the impact of denial of service attacks.
- **Privacy** – Information that can be used to identify network devices should not be available to unauthorized parties. This reduces the risk of intruders being able to map the network.

Infrastructure Layer, Control Plane Threat Model

This plane is concerned with securing the signaling information that resides on the network elements and server platforms.

The following controls should be addressed when analyzing the Infrastructure Layer, Control Plane security:

- **Access Control** – Network devices should only accept control information messages from authorized network devices – this reduces the threat of unwanted modifications. There also helps prevent worms from using control information to reconfigure the infrastructure and causing a denial of service.
- **Authentication** – The identity of the device sending control information should be confirmed. This control works in conjunction with access control to protect against unwanted changes.
- **Non-repudiation** – Maintain records that identify devices sending control information. Any modification should be recorded with the identity of the issuer, ensuring accountability for any changes to the infrastructure.
- **Data Confidentiality** – Control information includes data that is considered confidential such as passwords and security configuration details. To avoid third-party access to control information, data should be protected.
- **Communication Security** – Ensure that control information flows only from the intended source to the specified destination. Intruders may try to stop or capture signaling information to cause a denial of service.
- **Data Integrity** – Protect control information stored in network devices in transit or held at the servers. Intruders may attempt to capture control information in order to reconfigure the network elements.
- **Availability** – Ensure that network elements are always able to receive control information. Intruders may try to cause a denial of service by flooding the authentication server or other critical systems.
- **Privacy** – Information that could be used to identify a specific network element should be kept confidential.

Make Secure IP Video a Reality

Despite the ingenuity of fraudsters and hackers and the vulnerabilities associated with a relatively new technology, secure IP Video is a viable and rapidly growing technology as long as the requisite security technology remains current. Constant updating of the technology is required as fraudsters continue to implement new forms of attack.

The implementation of comprehensive security practices and processes can mitigate the risk involved and allow IP Video to take its place as a new and dynamic service to businesses and consumers.

Author

David Ramirez

Senior Manager, Global Practice
Security & Business Continuity

David was born in Colombia, he has been involved with Information Security for the past ten years. He began his career at Cyberia as networking specialist. Subsequently he joined KPMG managing the Information Risk Management practice implementation where he was involved in risk assessments for more than 80 companies. In 2002 David transitioned to DVS International Risk Managers as part of their new Information Security division. In DVS, David was responsible for developing the methodologies for the practice, covering Penetration testing and ISO 17799 compliance including disaster recovery. In this period he was involved in security projects for Banco Santander (Latin America), HSBC (Middle East), Lloyds Bank (Latin America), Barclays Bank (Spain), and other financial institutions in South Africa, Italy, Malaysia, USA and Central Banks in Italy, Turkey and Colombia; most projects in the areas of Security Awareness, Disaster Recovery & Business Continuity, Security Policies, Security Architecture, Managed Security Services and compliance with international standards.

David recently joined Lucent's Security & Business Continuity global practice; his responsibilities include supporting the EMEA and CALA regions. David holds several industry certifications including CISSP, CISM and BS7799 Lead Auditor; and technology certifications including MCSE:Security and ISS Certified Engineer. David is in the last stage of his MSc on Information Security at Westminster University London.

To learn more about our comprehensive portfolio, please contact your Lucent Technologies Sales Representative.

Visit our web site at www.lucent.com.

This document is for planning purposes only, and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to these products or services. The publication of information in this document does not imply freedom from patent or other protective rights of Lucent Technologies or others.

Copyright © 2005
Lucent Technologies Inc.
All rights reserved

XXX v1 09/05

Lucent Technologies
Bell Labs Innovations

