# D’Amo

## Comprehensive Database Encryption Solution

**Jane Elizabeth Keeler**
pspg@pentasecurity.com
January 2012

Penta SECURITY

Methods of communication, interaction, commercialization, health care, and governance are becoming ever more technology-focused in our modern age.  Documents such as medical records, tax and financial records, school transcripts, customer data, proprietary information, and all records containing personal identification data (such as name, date of birth, social ID number, etc.) were once securely and physically stored in paper form on-site in the locations where they were created, whether hospital, bank, university, business, or government office. Information security depended on safes, vaults, locked doors, and security guards. While such devices still play a role in modern security, the realm of information security continues to become ever more electronic. Instead of storing physical paper files containing personal data, such information is now, more often than not, maintained in electronic databases.

While the advent of the electronic database has enabled rapid data location and recall, as well as high-speed information sharing, it has also enabled the criminal element to access personal data – something they can at times do far too easily. Through various hacking techniques such as malware, theft of credentials, phishing, etc., hackers are able to gain access to private data stored within electronic databases, causing literally billions of dollars in damage per year. The damage caused by such hackers can be drastically reduced by encrypting valuable data, such as personal identifiers or confidential information – so why isn't encryption commonplace?

There are a number of factors that limit an organization's willingness to apply a database encryption solution, the most common factor being the erroneous belief that a database that is not directly connected to the internet is thereby protected from data breaches. In reality, however, just because a database is not directly connected to the internet does not guarantee its safety; all it takes is one database user infected by malware or one set of stolen credentials to allow an unauthorized user access to untold quantities of valuable data. Even when companies, organizations, and governments realize the threats posed by unencrypted data, they remain hesitant to employ an encryption system, often due to the notion that an encryption system is too complicated and difficult to use, and the worry that encryption will degrade system performance.

In contrast to such common misconceptions, D’Amo, a comprehensive database encryption solution from Penta Security Systems, Inc., offers a secure and easy-to-use method of encryption compatible with Oracle, MS SQL Server, DB2, MySQL, and SAP. D’Amo enables encryption of only the specific columns containing personal, proprietary, or confidential data, thus vastly reducing incidents of system degradation related to encryption. D’Amo’s patented Index Column Encryption Method enables high-speed searching of encrypted columns to help keep performance speeds high. Additionally, D’Amo’s access control policies and separation of roles between the Security Administrator and the Database Administrator help to secure the database against internal breaches.

## A Lack of Protection

According to the 2010 Independent Oracle Users Group Data Security Report, which surveyed 430 Oracle users, the main causes of database breaches were SQL Injection, malware, and stolen credentials. However, only a third of those surveyed stated that their organizations had taken steps to block SQL attacks. Additionally, fewer than 30% of companies surveyed encrypt the personal data in their databases, 75% lacked proper database access controls, and only 50% considered database security a ‘high priority’ in terms of IT security. The financial costs of data breaches can be huge, and loss of public trust can be devastating. Well-known corporations have recently fallen victim to database breaches, leading to much publicity surrounding this topic, so why aren’t more organizations utilizing database encryption solutions to protect their data?

*“Some data managers feel that their data is secure mainly because databases are not connected to the Internet—a false comfort that may lead to a rude awakening, especially considering that a majority of organizations admit that they do not apply Critical Patch Updates intended to address security vulnerabilities in a timely manner, or take steps to ensure that all their Internet-facing applications are not subject to SQL injection attacks.”*

**~2010 Independent Oracle Users Group Data Security Report**

# A Common and Expensive Threat

Despite the fact that many companies feel secure in their current database setups, 2011 has been a big year for database hackers. According to the Identity Theft Resource Center’s 2011 Breach List (released 22 November 2011), there were nearly 27 million confirmed records breached in the United States just this year, with an unconfirmed number of records breaches which could, if confirmed, cause that number to double. The Identity Theft Resource Center defines a ‘records breach’ as “an event in which an individual’s name plus Social Security Number (SSN), driver’s license number, medical record, or a financial record/credit/debit card is potentially put at risk.” The 2010 US Cost of a Data Breach study, released in March 2011 by the Ponemon Institute in conjunction with Symantec, states that the cost of a data breach has increased for the fifth year in a row, costing companies approximately $214 per record on average. That amounts to nearly six billion dollars (USD) in confirmed losses resulting from data breaches in the United States alone during 2011.

Some of the most well-publicized database hacks of 2011 included HBGary Federal, RSA, Epsilon, and Sony. HBGary Federal, a technology security company that contracts for the US Federal Government, had one of its databases hacked via SQL Injection, leading to the compromise of 60,000 confidential emails, as well as the social media (Facebook, Twitter, etc.) accounts of HBGary’s executives. Databases containing proprietary information about IT security solution provider RSA’s SecurID tokens were hacked when malware was introduced into their system via a phishing email. Marketing giant Epsilon had its email databases raided, releasing private email addresses of an undisclosed number of its corporate clients. Hackers were able to penetrate three databases belonging to media giant Sony, compromising 100 million customer accounts and 12 million customer credit card numbers. Sony has since spent over $170 million on system repairs and improvements, customer reimbursements, and legal costs.[1]

[1] Chikowski, Ericka. Five Infamous Database Breaches So Far In 2011. Security Dark Reading. http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229700130/five-infamous-database-breaches-so-far-in-2011.html Published 27 May 2011. Retrieved 30 November 2011.

SONY
SONY ONLINE ENTERTAINMENT
EverQuest
BUY NOW
SOE ALL ACCESS
RSA
EMC²
Advanced Persistent Threats Go Mainstream
HBGary
epsilon
Consumer Alert: Steps to Protect Your Email and Personal Information
Find Out What We Can Do for You 1.800.309.0505

Sony, RSA, HBGary Federal, and Epsilon were victims of some of the most well-publicized database hacks of 2011.

## Regulatory Compliance

Across the globe, governments and other regulatory agencies have begun to realize the potential value that personal data can have to hackers, and have started to implement laws and regulations pertaining to the control of such data.

**Sarbanes-Oxley Act,** (USA, 2002) – increased company responsibilities regarding accounting, auditing, and financial disclosures, as well as maintenance of information pertaining thereto. Similar laws have been passed around the globe, including the European Union's **8th Company Law Directive** and Japan's **Financial Instruments and Exchange Law**. Fines for violations can go as high as $5million USD, depending on the country and the nature of the violations.

**Health Insurance Portability and Accountability Act** (HIPAA, USA, 1996) – HIPAA's Privacy Rule tightly regulates the use and disclosure of medical records, amended in 2009 to include the **Health Information Technology for Economic and Clinical Health Act** (HITECH Act) which implemented strict new breach control and reporting requirements. Similar laws include the Australian **Health Records Act** and the European Union's **Recommendation on the Protection of Medical Data**. Fines for violations of such regulations have reached as high as $4.3million USD.

**Payment Card Industry Data Security Standard** (PCI DSS, 2004) is an international information security standard for companies dealing with electronic payment transactions (credit cards, debit cards, etc.), which requires secure management of cardholder data. Fines for violations can range from $5000-$100,000 USD per month.

**Federal Information Processing Standard** (FIPS) is a set of standards required by the United States Federal Government for use in computer systems used by government agencies and contractors. Well known FIPS standards include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). The international equivalent of FIPS is the **International Organization for Standardization** (ISO).

Other well-known privacy laws in place around the globe that regulate the maintenance and disclosure of personal information include the European **Directive on Data Privacy**, the Japanese **Personal Information Protection Law**, the South Korean **Act on Protection of Personal Data**, and the Australian **Privacy Act**.

*“Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to ‘decrypt’ it to obtain the original message.”*

**~Parliamentary Office of Science and Technology of the United Kingdom**

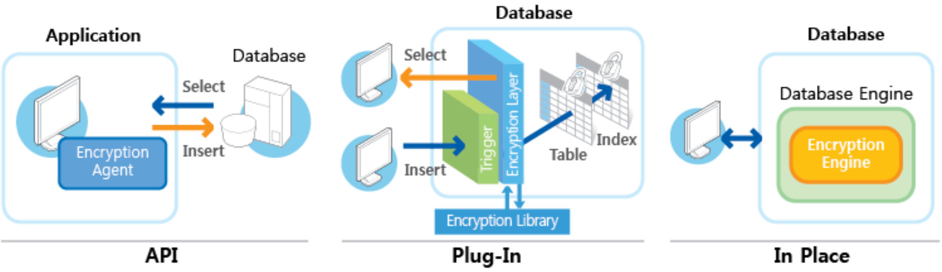
## D’Amo Product Line-up and Encryption Methods

Database encryption is generally divided into three methods: Application Programming Interface (API), Plug-In, and In Place (also known as Transparent Data Encryption, or TDE).

With API, data is encrypted on the application. As such, this requires modifications to all applications related to encryption target data. D’Amo SCP is the only member of the D’Amo product line-up to use this method. The API method can be supported on all databases, and encryption and decryption with this method do not place a load on the DBMS server. However, queries related to the encrypted target data must be modified.

The In Place (or TDE) method includes an encryption engine within the database engine itself, for the purpose of supporting rapid encryption and decryption, and allowing for complete independence from the application. Penta Security Systems, Inc. can work cooperatively with database vendors to design a database-specific In Place D’Amo system. Currently only D’Amo for ALTIBASE and D’Amo for MySQL support the In Place method. (D’Amo for MySQL is currently in production; Penta Security Systems, Inc. anticipates its release in January 2012.)

The Plug-In encryption method involves the installation of an encryption module on the database via plug-in. This method enables independence from the application, and requires only a minimal amount of query modifications. This method of encryption enables a support index for encrypted columns, and allows for comprehensive security, encryption, access control, and auditing. The majority of D’Amo products utilize this method, including D’Amo for Oracle, D’Amo for MS SQL Server, and D’Amo for DB2.



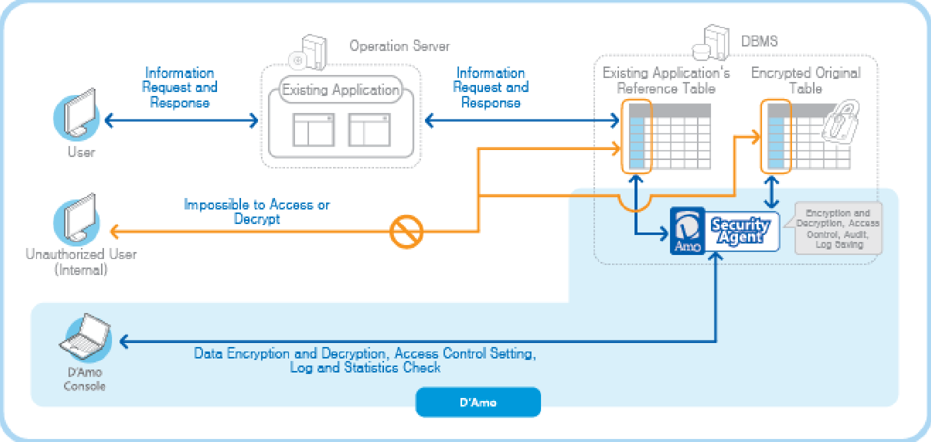
Penta Security Systems, Inc. also offers D’Amo for SAP, an encryption solution for SAP, which relies on the external D’Amo KeyManager hardware security module to configure and manage the encryption keys.

The D’Amo KeyManager is also available to support other D’Amo products if desired.

## Plug-In Database Encryption with D’Amo

Merely separating a database from the internet does not ensure that it will be free from breaches, as all it takes is one compromised computer with access to the database to leak its entire contents. Once a database has been breached, the only protection available for the data within is encryption. Securely encrypted data cannot be leaked, even if the database in which it is stored is breached.  When compiling its 2011 Breach List, the Identity Theft Resource Center did not count databases that had been breached but contained encrypted data as ‘security breaches,’ asserting that “When records are encrypted, we state that we do not consider that to be a data exposure.”[2]

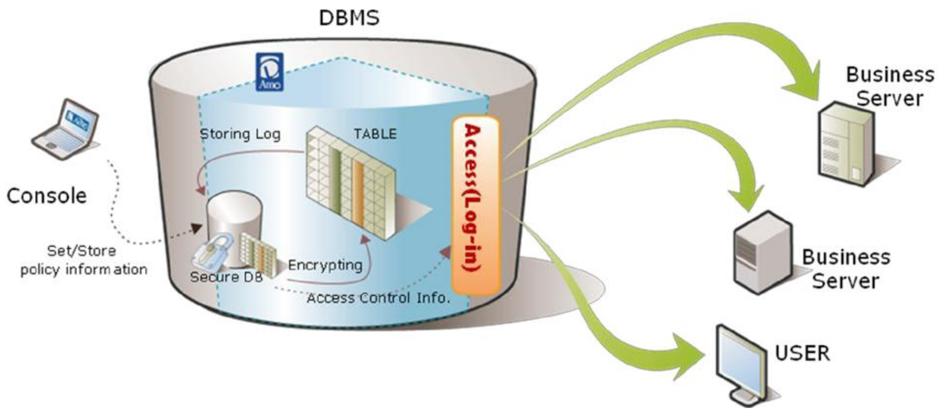
Many companies are hesitant to employ an encryption solution on their databases, due to a variety of concerns pertaining to post-encryption functionality. Encrypting an entire database can often lead to slow system performance, and a cumbersome and difficult to manage access process for legitimate users. D’Amo, the encryption solution from Penta Security Systems, Inc., is able to overcome these problems.


Operation Server
DBMS
Information Request and Response
Existing Application
Information Request and Response
Existing Application's Reference Table
Encrypted Original Table
User
Impossible to Access or Decrypt
Unauthorized User (Internal)
Amo
Security Agent
Encryption and Decryption, Access Control, Audit, Log Saving
D'Amo Console
Data Encryption and Decryption, Access Control Setting, Log and Statistics Check
D'Amo

D’Amo utilizes a **separation of authority** – often required to pass regulatory audits – to keep the roles and privileges of the database Security Administrator separate from the Database Administrator. The functions of D’Amo are designed to be utilized by the Security Administrator, whose responsibilities include creating and storing the ‘keys’ used for encryption and decryption, selecting which columns should be encrypted, and setting column access control privileges.

[2] Identity Theft Resource Center. 2011 Breach List. Page 79. http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf Published 22 November 2011.  Retrieved 30 November 2011.

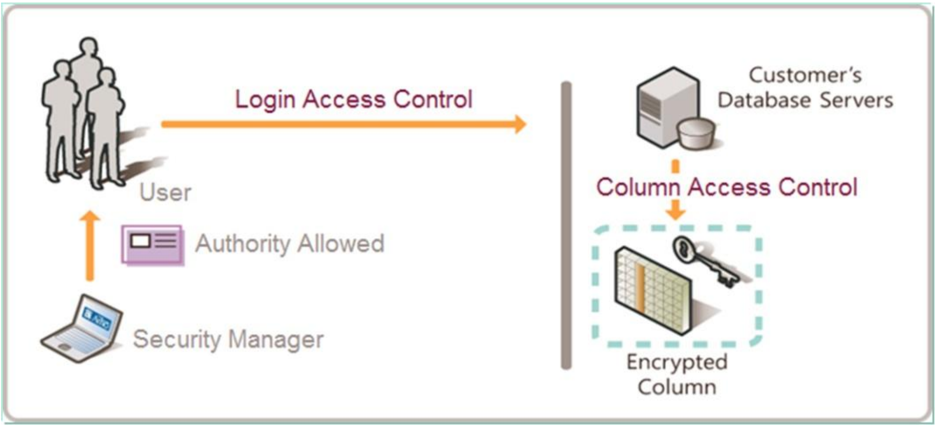
D’Amo is comprised of the **D’Amo Console** and the **D’Amo Security Agent**. The D’Amo Console is a user-friendly GUI console that allows the Security Administrator to easily perform encryption (or cancellation thereof), to configure and edit database and column access controls, and to access audit logs and database statistics. Multiple databases can be managed via the D’Amo Console. The policies that are established by the Console are encrypted and transmitted to the D’Amo Security Agent. The Security Agent is installed upon the databases secured by D’Amo. It performs the encryption/decryption, access control, auditing, and logging functions in accordance with the policies set by the Security Administrator in the D’Amo Console.



D’Amo offers the ability to **encrypt by column**. Conversely, decryption only occurs in when a privileged user queries an encrypted column, and only the specific column being queried is decrypted. Column-specific encryption and decryption enable the database to maintain its previous performance speeds and functionality while protecting vital data. Additionally, while other database encryption programs require changes to the application, tablespace, and/or string length in order to facilitate encryption, D’Amo enables encryption without any such changes. This reduces the overall administrator and system workload required for encryption and decryption.

D’Amo’s encryption and decryption processes are performed utilizing a **PKI-based symmetric key cryptosystem**. When establishing the encryption policies in the D’Amo Console, the Security Administrator can select from among the following algorithms for encryption: TDES, AES, SEED, ARIA, and BLOWFISH. Operation modes can be either

Cipher Block Chaining (CBC) or Cipher Feedback (CFB), depending on algorithm and administrator preference. The Security Administrator will also be able to select from the following options for initial vector: Fixed IV and Record IV. (For more on the algorithms, modes, and initial vectors utilized by D'Amo, please see Appendices A and B.) By use of its symmetric key encryption system and PKI based authorization, D'Amo is compliant with a wide variety of Korean, American, and international technology standards, a complete list of which can be found in Appendix C. Additionally, proper use of D'Amo enables companies and organizations to adhere to the various data privacy regulations set forth earlier in this paper.



Column-specific encryption and decryption functions – combined with D'Amo's **column access control** function – enable users with database access privileges, but who lack access privileges for encrypted data, to continue working in the database without any performance degradation. However, these users are unable to decrypt and view the original data for which they lack access privileges. Additional database **access control policies** can be configured based on IP/MAC address, login time, and application.

The Security Agent creates **event logs** for all SELECT, UPDATE, INSERT, and DELETE tasks in accordance with the policies configured in the D'Amo Console, as well as for all encryption and decryption events. These logs can be queried via the D'Amo Console. The D'Amo Console itself maintains the **policy logs** pertaining to encryption and decryption.

# Success of D’Amo: Nikon Systems, Inc.

http://www.nikon-sys.co.jp

## Profile: Nikon Systems, Inc.

Nikon Systems, Inc. is a subsidiary of the Nikon Corporation, founded in 1986 and headquartered in Yokohama-shi, Kanagawa, Japan. Nikon Systems, Inc. is a technology research and development firm that focuses on algorithm development and equipment control software. Their work deals with image processing (including the firmware for Nikon digital cameras), system integration, electronics, and documentation.

## Needs of Nikon Systems, Inc.

- Compliance with regulations implemented by the Japanese Personal Information Protection Law and the Japanese Financial Instruments and Exchange Law without the need to modify their pre-existing MS SQL Server system
- High level access control configurability and log management functions
- Prevention of corporate espionage and/or loss of proprietary data
- Specific target data for encryption: employee data such as names, telephone numbers, addresses, performance ratings, etc., as well as confidential proprietary data

**Nikon Systems, Inc. chose to install D’Amo for MS SQL Server, as it enables compliance with Japanese privacy laws, while performing the needed functions of encryption, access control, and log management in the MS SQL Server environment.**

## Results of Installing D’Amo

- Nikon Systems, Inc. had no difficulty integrating D’Amo into their pre-existing MS SQL Server environment, without having to modify their MS SQL Server database.
- Nikon Systems, Inc. has suffered no downtime or degradations in system performance as a result of applying encryption via D’Amo.
- Nikon Systems, Inc. is now in compliance with both the Japanese Personal Information Protection Law and the Japanese Financial Instruments and Exchange Law.
- Confidential proprietary data is now protected against data leakage, whether accidental or via corporate espionage.

*"Now I am relieved, due to a reliable data security solution.“*
~Nikon Systems, Inc. Data Security Representative

# D’Amo: The Comprehensive Database Encryption Solution

A company’s database is one of its most priceless assets, containing a wealth of personal, proprietary, and confidential data. Even the most physically secure systems can still be breached by threats such as malware or the trickery of phishing emails. Sometimes the leaks spring from within an organization itself, either intentionally or due to employee error. Once the system has sprung a leak, the only way to ensure that the data remains secure is via encryption. An encrypted system can be further enhanced with access controls and a separation of roles between the Security Administrator and the Database Administrator.

D’Amo, the database encryption solution from Penta Security Syaytems, Inc., offers all of these things. Internal security is enhanced by the separation of roles between the Security Administrator and the Database Administrator, as well as through the variety of login and column access controls that D’Amo provides. D’Amo enables encryption of only the specific columns containing personal, proprietary, or confidential data, instead of requiring that the entire database be encrypted, while its patented Index Column Encryption Method enables authorized users high-speed access. Additionally, when an encrypted column is queried by an authorized user, only that specific column is decrypted. Encryption and decryption by column help to drastically reduce the load placed on the system by encryption, enabling the system to operate efficiently. Use of D’Amo enables companies and organizations to achieve compliance with a variety of laws and regulations from around the globe, thus protecting their reputation, their customers, and their proprietary data, while avoiding data breaches as well as the fines and loss of customers which accompany them.

As long as valuable personal, proprietary, and confidential data exists, there will be those who will seek to access it for their own personal gain. Getting rid of such data is not an option, but storing it securely is. Encryption, coupled with access control and separation of duties, remains the best line of defense for valuable data. Don’t fall victim to a data breach: protect your database with D’Amo.

# APPENDIX A: Definitions of Algorithms, Modes, and Initial Vectors

**TDES** – Triple Data Encryption Standard, based on the DES (Data Encryption Standard) algorithm adopted by NIST in 1977. TDES overcomes the key length problem of DES by repeating it three times.

**AES** – Advanced Encryption Standard, an encryption algorithm adopted by NIST in 2001 as a substitute for DES.

**SEED** – Korean standard encryption algorithm developed in 1998 and approved by the Korean Telecommunications Technology Association in 1999.

**ARIA** – Korean standard block cipher encryption algorithm developed in 2003 and approved by the Korean Telecommunications Technology Association in 2004.

**BLOWFISH** – A symmetric block cipher encryption algorithm designed in 1993 as an alternative to DES.

**CBC** – Cipher Block Chaining, an encryption mode in which each block of plaintext is replaced (XORed) with the previous ciphertext before being encrypted. Used for ordinary block-based encryption.

**CFB** – Cipher Feedback, an encryption mode similar to CBC, but which transforms block cipher into a self-synchronizing stream cipher. Used for stream data transmission.

**Fixed IV** – Utilizes a fixed initial vector for encryption

**Record IV** – Utilizes a randomly generated initial vector for encryption

## Appendix B: D’Amo Algorithm, Mode, and Key Length Matrix

| Algorithm | Mode | Key Length |
|---|---|---|
| TDES | CBC | 168bits |
| AES | CBC, CFB | 128bits, 256bits |
| SEED | CBC, CFB | 128bits |
| ARIA | CBC, CFB | 128bits, 256bits |
| BLOWFISH | CBC, CFB | 128bits, 256bits |

## Appendix C: Technology Standards with which D’Amo Complies

- **FIPS 46-2, ANSI X9.52**: Replacement of the standard DES encryption algorithm that was developed by the US National Institute of Standards and Technology (NIST) with the TDES algorithm.
- **FIPS 197**: Advanced Encryption Standard (AES), announced by NIST in 2001
- **RFC4269**: SEED, a 128bit symmetric key block encryption algorithm developed by the Korean Information Security Agency in 1998
- **KS X 1213**: Korean Standard block cipher algorithm (ARIA), developed in 2003
- **RFC2459**: Public Key Infrastructure Certificate and CRL Profile
- **PKCS #1**: RSA Cryptography Standard
- **PKCS #3**: Diffie-Hellman Key Agreement Standard
- **PKCS #7**: Cryptographic Message Syntax Standard
- **PKCS #8**: Private Key Information Syntax Standard
- **ITU-T X.680, ITU-T X.690**: International Telecommunication Union Telecommunication Standardization
- **RFC2045**: Multipurpose Internet Mail Extensions (MIME), Format of Internet Message Bodies
- **FIPS 180-1**: Secure Hash Standard, SHA-1
- **FIPS 180-2**: Secure Hash Standards SHA-1, SHA-256, SHA-384, and SHA-512
- **ISO/IEC 9798-3**: Simple Authentication and Security Layer (SASL) Authentication Mechanism

- **RFC2104**: Keyed-Hash Message Authentication Code, HMAC
- **FIPS 113**: Computer Data Authentication Standard
- **ANSI X9.17**: Financial Institution Key Management Standard
- **IEEE P1363**: Institute of Electrical and Electronics Engineers Standard Specifications for Public-Key Cryptography

***Penta Security Systems Inc.***
*20th Flr., Hanjin Shipping Bldg., 25-11*
*Yeoeuido-dong, Yeongdeungpo-gu, Seoul,*
*Korea*
*Tel. 82-2-780-7728   Fax. 82-2-786-5281*

Penta SECURITY
www.pentasecurity.com