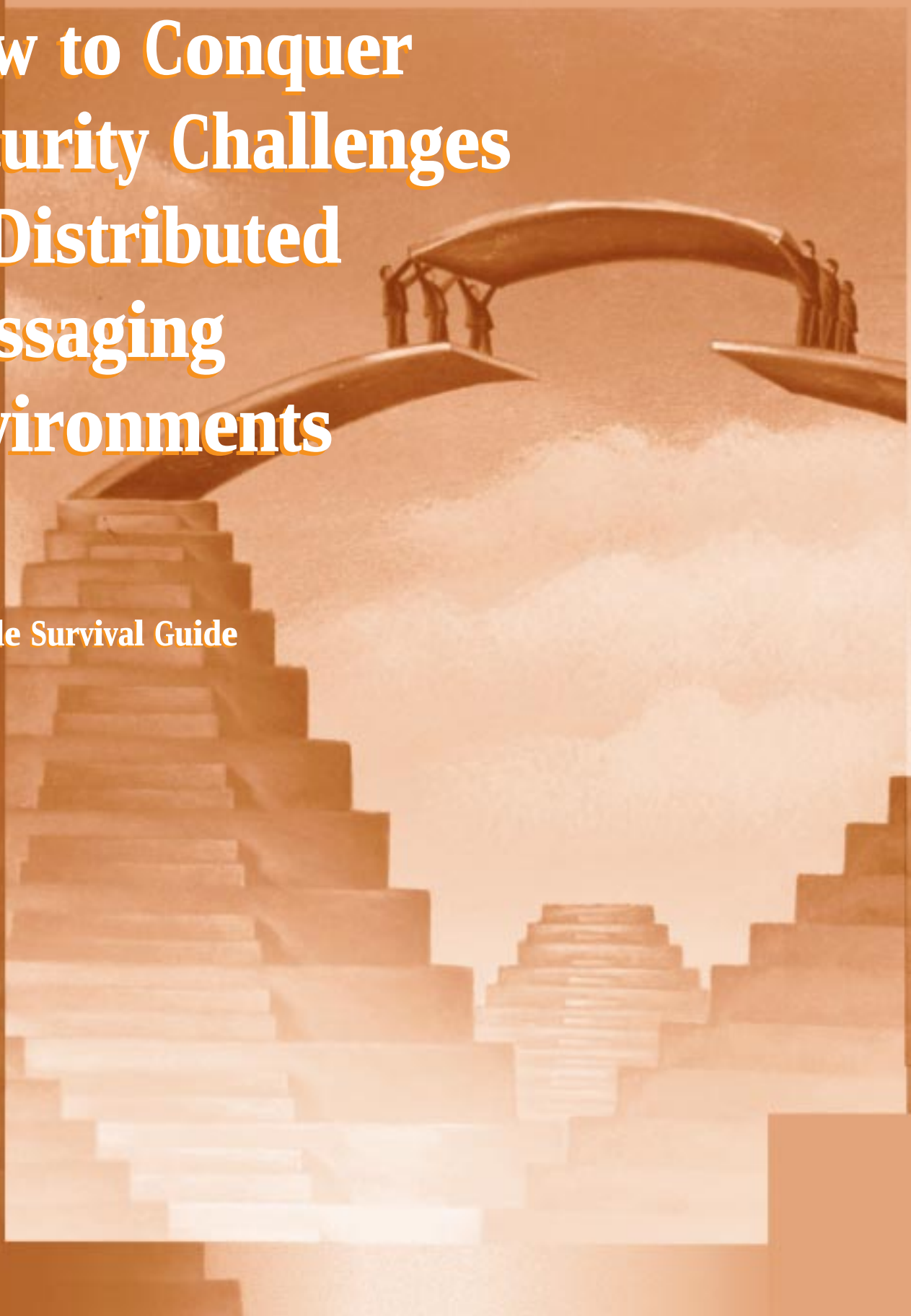
Candle®

How to Conquer Security Challenges in Distributed Messaging Environments



A Candle Survival Guide

The Risks of Open Access

The days of your banker recognizing you on sight and remembering you from a knee-high age are long gone. Now you're banking online, visiting the local ATM, and verifying transactions on a 24-hour hotline.

The business world is continually adopting new technology to stay competitive and to cater to increasingly technical markets and customers. Today, your business is involved in data processing, digital commerce, direct online communication with customers, and transferring information over distributed networks, such as the Internet.

In the beginning of the well-publicized Information Age and the coming of the Information Super Highway, we all discussed "access" and how to bring information to the masses. After a decade of amazing growth and expansion, we're starting to realize that the technology that's helping us conduct business faster and farther is also putting us at risk. The corporate lifeblood – information – can be exposed, stolen, misrouted, or altered. Your corporate liability can be enormous.

Why Worry About Security?

Why should you worry about security? Because a security breach will cost… time, money, data, your customers, your reputation, your business.

According to a study by the Federal Bureau of Investigation (FBI) and the Computer Security Institute (CSI), computer security breaches have increased steadily, resulting in approximately $137,000,000 in losses in 1998, up 36% from 1997. In addition, the security breaches are split almost evenly between external and internal attacks. The complete report, *Current and Future Danger* (for sale on the CSI website) illustrates trends and identifies the most common types of attacks.

One of the difficult aspects of quantifying computer crime is that companies that have been compromised go to great lengths to hide or deny a breach, since the negative publicity can do more damage than the initial break-in. In addition, many companies are unaware of an attack. In the Salgado case (the FBI apprehended Carlos Salgado with 80,000 stolen credit card numbers), two of the compromised companies were not even aware of a breach until the FBI contacted them for cooperation in the investigation.[i]

While the Salgado case revealed how lucrative hacking into corporate systems can be, it is not the only motivator for cyber crime. There are large, organized groups of hackers who specialize in exposing security holes and weaknesses. Some are looking for financial gain, some are looking for fame or political power, and some feel compelled to push the industry to keep improving security techniques. According to *Internet Week*, the number of hackers targeting e-commerce sites is on the rise and several online stores have recently shut down their sites after discovering hacker damage. Systems hacked for technological or political reasons include the Pentagon and the US Coast Guard. *Computerworld* and the AntiOnline, a website and organization dedicated to tracking security breaches, both reported that the Pentagon suffered a successful attack on non-classified data, while the US Coast Guard lost a sensitive database (costing $40,000 to replace) due to a break-in by a disgruntled former employee.

While some Information Systems professionals feel overwhelmed by the variety, quantity, and creativity of the attacks, it is NOT a solution to hope that your system will simply be overlooked by the hacker community or that every employee is 100% ethical. You can hire a security consultant – the industry (and the average consultant's salary) is growing at a phenomenal pace. You can purchase "Secure Systems Insurance" – an insurance policy against hacker damage. You can learn as much as possible about technology available to protect your business assets – which you're doing by reading this survival guide. By being informed, you can combine your knowledge with a solution for your business.

What You Need to Know About Security

You need to know the risks and liabilities of your business. The threats to your company's information are real and can range from reasonably innocent errors and glitches to malicious hacking. Just as you purchase virus-protection software to prevent and solve problems BEFORE there is damage to your data and system, you need to proactively invest in ensuring the security of your data.

In an MQSeries™ environment, several different platforms communicate application commands and your company's critical information through message queue managers. Since messaging is the transmission of technology (data, email, strings, objects) from one system to another across machines or platforms, the "message" becomes the object that must be secured. Begin educating yourself on security issues for your messaging system.

Who's on the system?

Identification is the ability to verify single users or entities by their unique characteristics. This can mean a server's ability to verify a user by a unique login and password. Perhaps your company provides each employee with a unique numeric key to enter the building. Any process through which you confirm a single individual entity is identification. Identification is the very first piece of security; you must know with certainty each user or entity in your system.

Control Access to Data & Systems

A very large component of Information Systems and Network Administration work is access control. IS professionals routinely limit user access to commands, applications, servers, and networks based on security privileges and work needs. You need to know that the ability to send a change-data message to your corporate database is granted only to identified data-entry clerks with proper training and clearance.

What is Authentication?

In a messaging environment, identification must be followed by authentication. Authentication is the ability to verify that a message or transaction actually came from the individual entity claiming to have sent it. For example, your company is involved in an acquisition and plans to transfer funds from your bank to the bank of the company from which you're purchasing a new subsidiary. The two banks must undergo a process of identification and authentication. First, they should verify that both are legitimate and the bank they claim to be. All messages between them then have to be authenticated to prove that they were genuinely sent by the other bank.

You Must Assure Data Integrity

Say that, in the process of transferring the funds for your acquisition, your bank sent a message indicating the transfer of $100,000 to the receiving bank. Imagine your surprise when your next statement shows the transfer of $100,000,000! The addition of three zeros is not a large change in the size of the message, but is a very large change to your bottom line. The ability to deliver data exactly as it was sent, with the assurance that the data has not been altered, is critical. This includes a verification step when a message is received to check the message for signs of alteration. This is known as data integrity or data verification.

Minimize Liability, Increase User Accountability

Non-repudiation is the ability to prove authorship of messages and transactions. This prevents denial of authorship and ensures both employee and customer accountability. As online customer transactions become more common, this verification becomes increasingly crucial. Non-repudiation protects your company from the customer who denies sending a message to change his stock portfolio just prior to a market "correction."

Confidentiality Through Encryption

A message is considered confidential if it is read only by the intended recipient. One way to assure the confidentiality of messages is to render plain text unintelligible by passing it through an algorithm that converts text into "cipher." The message can be deciphered back to plain text only by using the proper key. Encryption is the process of converting plain text into unintelligible text. In your business, encryption can be used to assure the confidentiality of sensitive data. For example, customers ordering your product through the Internet expect that their credit card numbers, at a minimum, will be encrypted and kept confidential.

Define Your Business Needs

As you learn about security, think about your risks. What would happen if you lost some or all of your corporate data? What would happen if you violated the confidentiality of customer information? What would happen if the data entry for one week was corrupted, intercepted, or altered?

It is critical that you perform an internal risk assessment so you can make an educated decision about how to protect your company. Once you define the area of your greatest risk, you can match that with a security solution that offers the maximum protection for your business.

Evaluate your business and identify areas of concern such as databases of confidential data, personnel access, data that must cross distributed networks, and communication with remote employees, customers, or businesses. Take a moment to make notes about

where your sensitive information resides or travels and what the access points to that data might be. There are different security strategies for businesses that conduct transactions within their own network and those that have broader processing activities.

MQSeries offers some opportunities to plug additional security into the messaging environment. As middleware that helps your company communicate across a variety of platforms and applications, it provides an open architecture in which to customize your security solution. For example, in MQSeries, you can write your own exits or use a third-party product that has already coded the exits to provide authentication, message integrity and/or encryption. DCE exits are supplied with MQSeries, but require an implementation of DCE. These exits provide you with a framework for internal network security from server to server.

Secure Servers and Queue Managers

Node-to-node, or narrow, security describes security measures from one node (server or queue manager) to another. Once a node is authenticated, messages from that node and communication between two authenticated nodes is considered secure. In this manner, a communication channel can be considered secure. MQSeries can handle node-to-node security through custom, third-party, or DCE channel exits.

Example: A remote office of your company handles all data entry for your customer orders. In the node-to-node model, the channel of communication from that office is authenticated and the messages transferred to your office are considered secure as they travel between the systems.

Secure End Users and Applications

Known as end-to-end or broad security, this describes security measures from end user or application to end user or application. The user is authenticated and messages from that user can be considered secure. In addition, messages are protected from the end user, through the channel, in queues, all the way to the destination end user or application.

Example: In the remote office that handles all data entry for your customer orders, the transactions from each clerk are authenticated and the message data is protected from the clerk to that node, in transit to your node, in your queue, and to your end application.

Write Your Security Spec

Consider the way you do business and where your sensitive data resides and travels. If your sensitive data stays within the confines of internal, authenticated nodes where secured sessions have a high level of reliability, MQSeries node-to-node with DCE encryption installed may offer enough protection. If your sensitive data travels beyond the queue manager nodes, consider investing in end-to-end security solutions. If DCE is not your first encryption choice, investigate alternative third-party security solutions. For detailed information about current security issues (inherent security, opportunities for external security, and areas identified for increased security in the future), consult the *MQSeries Security White Paper*.[ii]

Think about each of the security concepts and how you are currently addressing them. Do your employees understand the importance of secret and unique passwords to identify themselves? Do you have adequate methods in place to authenticate your users? How frequently are they (and do they need to be) authenticated? Would your current system allow customers to deny sending messages or claim they had been sent or altered without their knowledge? Does your IT department actively manage user access conservatively or does it default to wide-open permissions and scale back only after problems? Do you encrypt any communications? Should you? Could you be encrypting too much and slowing down your transactions unnecessarily? Would you know if a message was altered? Ask yourself the tough questions – the answers are the product specification for your security solution.

How to Evaluate Security Offerings

Once you have identified your needs and areas of risk, you can prioritize security features for your business. The purpose of this section is to highlight the subtleties that distinguish security offerings on the market and to discuss the advantages and disadvantages of some features and approaches.

Authentication

The mechanisms of authentication offer different degrees of protection. Authentication can mean that the system can “prove” that the message or transaction has a given user identifier – without the ability to tie that identifier to the station or user.

MQSeries authenticates by “passing user context,” which sends the user id and password with the message in plain text. This method is adequate where the network is not prone to any interception or “eavesdropping,” but means that any interception provides the hacker with a valid user id and password into your system.

Authentication can also be handled outside the software application – such as network login or building security for the authentication. This method is only as good as the control on the secondary technology. The US Coast Guard breach, for example, was compromised by a disgruntled former employee using the active user id and password of an employee who shared this "unique and secret" information with co-workers.

There is also a range in frequency of authentication – some applications require authentication only at start-up, whereas others offer authentication on every transaction. Since the method some hackers use to access systems is to dial in to active machines, it can be unwise to assume that an authenticated machine will remain secure.

Non-repudiation

Non-repudiation is only as good as authentication. Look carefully at a software solution's ability to authenticate end-users, because that may be where your greatest need for accountability lies. Especially in environments with data entry of sensitive material or direct customer access, non-repudiation to the level of the individual may be necessary to minimize your business liability.

Data Integrity

In the banking example given earlier, the smallest alteration (adding "000") had huge impact on the result of the data message. While this seems the simplest level of security, it should not be overlooked.

Find out how data integrity is verified. The message size may be checked before and after transfer. Many security solutions convert content to a mathematical equivalent and send the resulting value along with the message. The value is recalculated by the recipient and checked against the one sent with the message. This method will not catch any alterations to the message that do not impact the file size.

Other methods use both content and additional information, such as user id, to create the mathematical equivalent. Investigate the thoroughness of the data integrity check, also keeping in mind that the check will be performed wherever your security is implemented, such as upon channel exit or at the end user or application. An integrity check at the channel exit will verify that the message was not altered between nodes, but will not tell you anything about what happens from the node to the end-user.

Confidentiality / Encryption

There is a huge variety of options within the realm of encryption. Encryption is the process of converting plain text into undecipherable characters. Many methods are available, but all include overhead in expense, security, and speed.

Secret-key or "symmetric" encryption uses one key to both encrypt and decrypt data. This method works well with small groups and is very fast, but is very difficult to keep secure when large numbers of users are sharing a single key that must be delivered to new users across communication channels. The federal standard in secret-key encryption is DES. Developed by IBM in the 1970's, it is not considered robust enough for today's security demands and is scheduled to be replaced by the Advanced Encryption Standard (AES) in the next few years.[iii]

Public-key encryption was created to allow encryption among larger user groups and distributed networks. Each user has both a public and a private key. The public keys are distributed, while private keys are unique to individuals and are not shared in any fashion. A public key and the sender's private key are used to create a digital signature on a message. The recipient uses a public key to verify the digital signature and his or her private key to decrypt the message. RSA (Rivest, Shamir, and Adleman) encryption was developed to answer the need for increased security among large user groups and is the most popular public-key encryption in use today.[iv]

Encryption methodology is a major factor in data-integrity and non-repudiation. If any portion of a transaction or the user id is encrypted, the method can become the loophole through which a sender can deny authorship or changes can be introduced. In secret-key encryption methods, for example, both sender and user must have an identical secret key. Short of physically handing the key from one to the other, there must be a courier to transport the key. If the courier uses the key to alter a message, data integrity is lost. Even if the courier does NOT use the key, either party can claim that a message was compromised by the courier.

The strength of the encryption is critical. Strength is based on the difficulty of breaking or deciphering a message or key. The hash function that reduces messages to a fixed length, the algorithm (such as a block or stream cipher) that encrypts the message and digital signature, and the key length, all affect the strength of the encryption. The security of the method increases with the key length; the larger the number of bits, the greater the possible combinations and the harder the key is to discover. Currently, the US government limits the export of encryption methods to 40-bit keys (with some exceptions), but encryption within the US typically uses 56-bit or 128-bit keys.

As you evaluate security solutions, check into the encryption options: must all of every message be encrypted, or can you choose portions? Encryption requires space and time, so encrypting unnecessarily slows down your transactions and your whole business. For example, your company conducts online ordering with direct customer access. You might choose not to encrypt the items the customer is ordering from your catalog, but choose to encrypt customer name, address, and credit card number. This will significantly decrease the overhead of the transaction without compromising the confidentiality or security.

Secure Servers and Queue Managers

This is the basic level of security. Since it may be all you need, find out how it's implemented by the solutions you consider. Do not assume that all node-to-node security is created equal. Look for frequency of authentication and your ability to customize. You have the choice between products that establish "trusted" nodes and those that offer authentication for each transaction. You should also evaluate the security of your architecture and how likely it is that a "trusted" node could become untrustworthy or be accessed by an unauthorized user. You may want the option of both or the ability to use a hybrid solution to fit your needs.

Secure End Users and Applications

If, in evaluating your risks and security needs, you decide that end-to-end protection is prudent for your business, choose a security solution that can offer this implementation option. End-to-end can protect messages from one end application to the final destination and in every stop along the way. Some security solutions cease protection before the final destination, such as in a server queue. Messages often stay in queues for an extended period of time, providing a prime opportunity for data to be accessed and compromised by an internal or external hacker.

As online commerce and public network transactions become more common, this feature is becoming imperative. The lack of end-to-end security can be a barrier to companies on the verge of taking their business to the next level of customer service and transactional efficiency.

Available Solutions — MQSecure

Among the security solutions on the market today, Candle Corporation offers MQSecure™ for MQSeries™ environments.

The versatility and thoroughness of the product have earned it a "Flying Colors" award and the "Editor's Choice for Best Message-Oriented Middleware (MOM) Security" award from *Network Computing*, as well as a very favorable review in the *Hurwitz Report Tool Spotlight*.

Authentication

MQSecure does not rely on building security or login for user authentication. Instead, MQSecure assigns each message a digital signature based on user id and a message digest (created by the mathematical representation of the content). The same method is used to authenticate nodes and end users or applications.

Authentication can be performed on EVERY message or only on start-up of the node or end-user system. Authenticating every message prevents an unauthorized message or user from violating security by using a "trusted session" to obtain data or send false messages. Authentication on start-up may be all that's necessary in secure internal networks with reliable trusted session environments.

Non-Repudiation

Because MQSecure can be configured for node-to-node or end-to-end security, non-repudiation is available at the end-user level. In the example of a brokerage firm or bank allowing online transactions, MQSecure can provide user-level non-repudiation to minimize your company's liability by ensuring user accountability.

Data Integrity

Data is validated by MQSecure by creating a message digest encrypted with the sender's private key. The resulting digital signature accompanies the message to the recipient. The recipient uses the public key to decrypt the signature, create a message digest and compare the resulting digest with the original. If there is a match, the message is valid, and is considered unaltered. If there is even the slightest change to a message or signature in transit, the message digest cannot match and the message is invalid.

Depending on the configuration, data integrity can be validated by MQSecure at the queue managers or end applications or users. The integrity of the data is validated wherever MQSecure is implemented.

Confidentiality / Encryption

MQSecure utilizes RSA encryption. In addition to the advantages of a public-key encryption method, RSA is widely deployed, making support and implementation easier and more cost-effective. Custom solutions or specific high-end algorithms could add to your implementation costs. In addition, the encryption can end up becoming a separate installation that requires support.

Since MQSecure uses RSA public-key encryption, no third party need be involved in any transaction. This eliminates the biggest loophole in secret-key encryption – in which there is integrity loss and plausible deniability by virtue of the courier of the key. With MQSecure, there is no transport of private keys and therefore any message can be traced to its unique and original public and private key combination source.

The "industrial-strength RSA encryption algorithm" used by MQSecure includes a 128-bit hash value expressed as a 32-digit string of hexadecimal digits. The message is encrypted with the sender's private key; then the message and message digest are encrypted with a public key. The result is decrypted with the recipient's private key, requiring that only public keys be distributed and offering strong encryption security. Candle Corporation has been granted the ability to export MQSecure with strong encryption outside the United States (with some restrictions).

MQSecure also offers selective encryption, which allows the user or administrator to choose partial or complete encryption of messages. This reduces the overhead necessary for encryption, but allows sensitive data to be protected.

Implementation Security Options: End-to-End or Node-to-Node

MQSecure offers complete customizability of node-to-node or end-to-end security implementation. End-to-end security applies to end users, and applications. If end-to-end is implemented, messages are protected in transit and in the message queue… anywhere in channel. In node-to-node implementation, MQSecure offers authentication on EVERY transaction. Node-to-node implementations can secure the network while remaining transparent to the users or be configured to offer the user explicit encryption options.

MQSecure Protected Platforms

Windows™ NT, Windows 3.1 (with a client connection), HP/UX, OS/2®, AIX®, and MVS. Contact Candle Corporation *(see following page)* regarding MQSecure support for Sun Solaris and Windows 95 and 98.

Feature Summary

Feature	Definition	Why is it important	How it is accomplished through MQSeries with MQSecure
Identification	Ability to verify a single entity by its unique characteristics	Provides knowledge of who & what can access the system so security can be controlled	IBM's MQSeries provides methods for user identification, MQSecure can utilize the user login and user id for identification.
Authentication	Ability to verify that a message came from a specific identified user	Keeps unauthorized messages from posing as legitimate messages	MQSecure can authenticate every message, which ensures that each message came from an authorized user.
Non-Repudiation	Ability to prove authorship of messages or transaction to prevent denial.	Minimizes liability; ensures employee and customer accountability for messages	MQSecure can authenticate every message from end-to-end, providing the ability to prove authorship to the end-user level.
Access Control	Ability to control user privileges and abilities within the system	Ensures that only authorized persons with proper training & clearance can access data	IBM's MQSeries provides tools to control user access and privileges.
Encryption	Process of converting plain text into unintelligible text	Allows messages to be transferred confidentially	MQSecure encrypts with RSA public-key encryption using a 56- or 128-bit key. MQSecure allows total or partial encryption at user or administrator discretion.
Data Integrity	Assurance that data is correct and unaltered	Prevents decisions or actions based on incorrect messages	MQSecure checks data using both public and private keys, an encrypted message digest, and a mathematical message equivalent.
Node-to-Node Security	Security measures implemented at the server level, protecting data inside the network	Protects messages within the network	MQSeries requires DCE for security at the channel exits. MQSecure uses RSA encryption and can implement any or all its features at the node-level if desired.
End-to-End Security	Security measures implemented at the user level, protecting data anywhere in a distributed network	Protects messages over a distributed network, between nodes and to and from the end users	MQSecure protects messages from the end user, in transit to the node, in the queue, from the node to the end user, and in the end-user's queue. MQSecure can implement any or all of its features to this level, if desired.

Candle World Headquarters

- Internet Address: www.candle.com
- Candle Corporation, 2425 Olympic Boulevard, Santa Monica, CA 90404, (310) 829-5800
- Europe - Candle GmbH, Munich, Germany (49) 89 5 45 54-0
- Australia/New Zealand - Candle Corporation, Sydney, Australia (61) (2) 9954 1500
- Asia - Candle Japan Corp., Tokyo, Tel. (81) (3) 5562-6991

  Candle Far East Ltd., Singapore (65) 220-5092

---

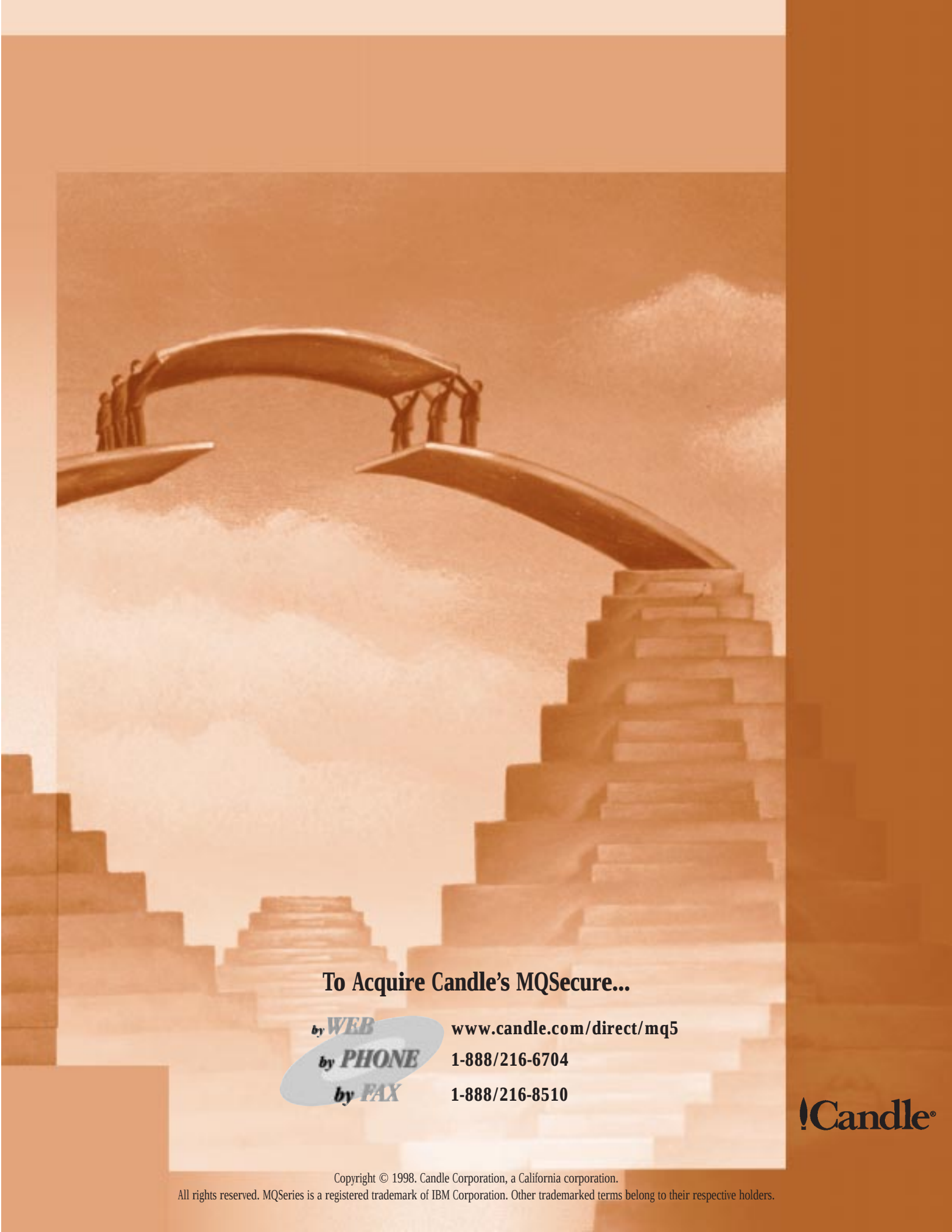
i "Special Report: Salgado case reveals dark side of electronic commerce" Richard Power, CSI Monthly Newsletter, September 1997.

ii "MQSeries Security White Paper" Stuart C Jones, IBM UK Labs, Last revision February 20, 1997, (www.software.ibm.com/ts/mqseries/txppacs/ms06.html).

iii "What is the role of the United States government in cryptography?" RSA Laboratories (www.rsa.com).

iv "What are some popular techniques in cryptography?" RSA Laboratories (www.rsa.com).

v "Hurwitz Report Tool Spotlight - June 1997" Steve Foote.



To Acquire Candle's MQSecure...

by WEB www.candle.com/direct/mq5

by PHONE 1-888/216-6704

by FAX 1-888/216-8510

Candle®