第一部分

基 础 篇

第 1 章 企业应用安全

当计算机将我们包围、当网络无处不在时，安全问题成为了我们日益关心的问题。我们依赖于网络，同时又受限于网络，而网络本身却是不安全的！如今越来越多的企业应用都架设在网络平台之上，虽然这样能为用户提供更快捷和便利的服务支持，但这些服务支持也越来越庞大。与此同时，为了满足用户日益增长的服务需求，企业应用不断在如何提供更好的服务支持和更大信息量的传输方面加大技术投入。而与此失衡的是，企业应用的安全性却未能受到足够的重视。单凭用户名和口令鉴别用户身份，继而授权用户使用的方式难以确保数据的安全性。

1.1 我们身边的安全问题

安全，似乎是个问题。但是，我们觉得这个话题似乎不是那么关键！通常情况下，我们通过为用户提供用户名和口令验证的方式就可以避免这个问题，但这不是最佳答案，因为这样做是远远不够的。安全隐患无处不在，还是先来看看我们所处环境的安全状况吧！

- 存储问题：闪存芯片的快速的、革命性的发展使得移动存储行业发生了质的变化，各种数据存储在各种不同的移动存储设备上。当塞满了公司的年度报表、下一年企划策略等各种商业机密的优盘突然不翼而飞时，我们才会猛然惊醒——优盘中的数据没有任何安全措施，甚至连口令都没有！
- 通信问题：我们习惯于通过IM工具与好友聊天、交换心情、透漏隐私，甚至通过IM工具与合作公司交换公司私密数据！当你的隐私成为公共话题时，或当你的公司的商业数据被曝光时，你突然发现原来IM工具是不安全的！没错，不管是哪一种IM工具，都在不遗余力地告诫用户聊天信息可能被盗取，“安全提示：不要将银行卡号暴露在您的聊天信息中！”相信大家都不会对这条提示信息感到陌生。
- B2C、B2B交易问题：到邮局排队汇款的日子已经一去不复返了，取而代之的是网上银行，轻松地点击一下按钮就能顺利完成转账的操作。网上银行的确为我们的生活带来了便利，但是，如果我们有被钓鱼网站骗取银行卡号和密码的不幸遭遇，那么现在想起来是不是仍然心有余悸？难道没有一种办法能确保我们输入的信息被发送到安全的

地方吗？

- 服务交互问题：随着大型应用对交互性的需求越来越高，这些应用之间的数据交互也越来越频繁，甚至是大批量、高负荷的数据交互。当你公司的应用通过Web Service接口与合作伙伴交互数据的时候，你该如何确定对方就是你所信赖的合作伙伴呢？你的Web Service接口安全吗？
- 移动应用服务问题：3G时代已经来临，在不远的某一天，你将完全可以通过手机完成现在只能通过PC完成的事情，如视频聊天、B2C购物、银行转账等等。3G时代预示着智能手机将无所不能！其实手机也是计算机，只不过它与你熟悉的PC在体积上有较大的差别而已。3G手机一样要通过网络完成你要执行的操作，将平台由PC转换为手机，并不能保证手机平台就能比PC平台有着更高的安全性！用手机在WAP网站上下载一款软件，是再平常不过的事情了。但是，如何避免用户因不够信任该软件而取消下载呢？下载后，手机如何鉴别这个软件是安全的呢？如何避免发布的软件在被客户成功下载之前被篡改呢？
- 内部人为问题：前面列举的问题都来源于外部，我们往往忽略了内部人为问题。现在的企业应用都能为用户提供用户名和口令来确保用户的数据安全，但很多时候用户名和口令在数据库中却一目了然，甚至有的是以明文方式存储的！企业内部任何能访问数据库的员工都能轻而易举地盗取用户的用户名和口令，然后冒充用户的身份完成各种合乎用户行为的操作，侵害用户的利益。企业因此被用户投诉之后，却又找不到任何蛛丝马迹。

当我们的利益受到侵犯时我们才会想起安全问题，安全原来如此重要！一不小心，你的企业应用就会因为数据泄露而丧失良机、引发投诉，甚至是付出巨额赔款！安全问题关系着企业的生死存亡！

1.2 拿什么来拯救你，我的应用

“拿什么来拯救你，我的应用？”这几乎是每一位架构师和安全工作者都会关注的问题。看了上面那么多让人不寒而栗的安全问题，免不了让我们心里发怵。魔高一尺，道高一丈，我们先来看看有什么武器可以应对企业应用的安全问题。接下来会讨论安全技术目标、OSI安全体系结构与TCP/IP安全体系结构这三方面的内容。

1.2.1 安全技术目标

国际标准化组织（ISO）对“计算机安全”的定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”根据美国国家信息基础设施（NII）提供的文献，安全技术目标包含保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可靠性（Reliability）和抗否认性（Non-Repudiation）。

- 保密性：又称机密性。保密性确保数据仅能被合法的用户访问，即数据不能被未授权的第三方使用。
- 完整性：主要确保数据只能由授权方或以授权的方式进行修改，即数据在传输过程中不能被未授权方修改。
- 可用性：主要确保所有数据仅在适当的时候可以由授权方访问。
- 可靠性：主要确保系统能在规定条件下、规定时间内、完成规定功能时具有稳定的概率。
- 抗否认性：又称抗抵赖性，主要确保发送方与接收方在执行各自操作后，对所做的操作不可否认。

除此之外，计算机网络信息系统的其他安全技术目标还包括：

- 可控性：主要是对信息及信息系统实施安全监控。
- 可审查性：主要是通过审计、监控、抗否认性等安全机制，确保数据访问者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，当网络出现安全问题时，提供调查依据和手段。
- 认证（鉴别）：主要确保数据访问者和信息服务者的身份真实有效。
- 访问控制：主要确保数据不被非授权方或以未授权方式使用。

安全技术目标制定的主旨在于预防安全隐患的发生。安全技术目标是构建安全体系结构的基础。

1.2.2 OSI安全体系结构

OSI参考模型是由国际标准化组织制定的开放式通信系统互联参考模型（Open System Interconnection Reference Model，OSI/RM）。OSI参考模型包括网络通信、安全服务和安全机制。网络通信共分七层，按照由下至上的次序分别由物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer）构成。其中，数据链路层通常简称链路层。国际标准化组织于1989年在原有网络通信协议七层模型的基础上扩充了OSI参考模型，确立了信息安全体系结构，并于1995年再次在技术上进行了修正。OSI安全体系结构包括五类安全服务以及八类安全机制。

OSI参考模型结构如图1-1所示。

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。

- 认证（鉴别）服务：在网络交互过程中，对收发双方的身份及数据来源进行验证。
- 访问控制服务：防止未授权用户非法访问资源，包括用户身份认证和用户权限确认。
- 数据保密性服务：防止数据在传输过程中被破解、泄露。
- 数据完整性服务：防止数据在传输过程中被篡改。

❑ 抗否认性服务：也称为抗抵赖服务或确认服务。防止发送方与接收方双方在执行各自操作后，否认各自所做的操作。

从上述对安全服务的详细描述中我们不难看出，OSI参考模型安全服务紧扣安全技术目标。

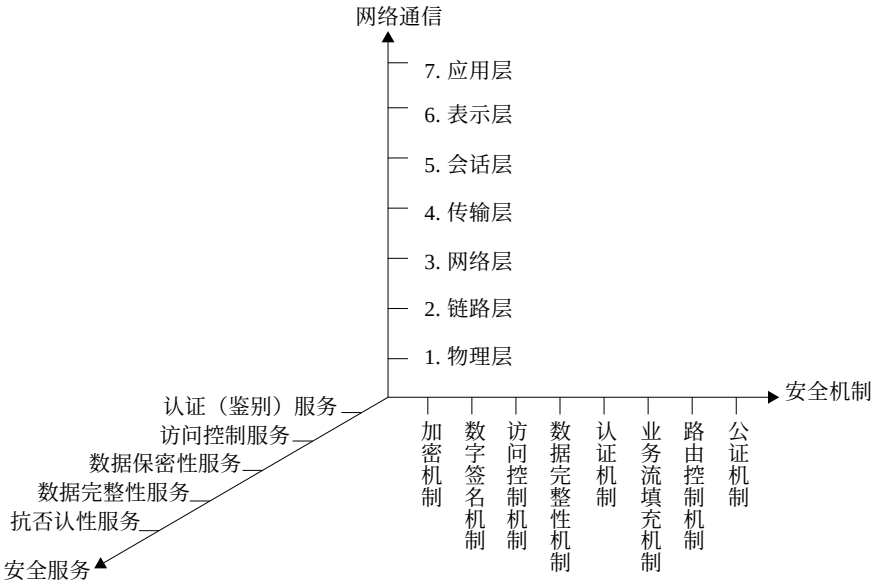

图1-1 OSI参考模型

安全机制是对安全服务的详尽补充。安全服务和安全机制的对应关系如图1-2所示。

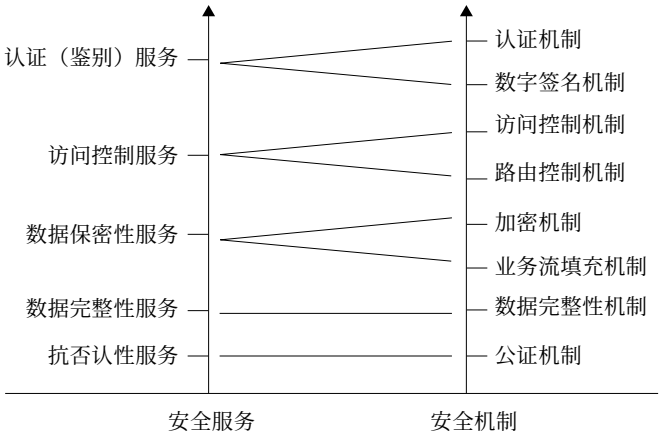

图1-2 OSI参考模型安全服务和安全机制的对应关系

八类安全机制包括加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制和公证机制。

❑ 加密机制：加密机制对应数据保密性服务。加密是提高数据安全性最简便的方法。通过对数据进行加密，有效提高了数据的保密性，能防止数据在传输过程中被窃取。常用的

加密算法有对称加密算法（如DES算法）和非对称加密算法（如RSA算法）。

- 数字签名机制：数字签名机制对应认证（鉴别）服务。数字签名是有效的鉴别方法，利用数字签名技术可以实施用户身份认证和消息认证，它具有解决收发双方纠纷的能力，是认证（鉴别）服务最核心的技术。在数字签名技术的基础上，为了鉴别软件的有效性，又产生了代码签名技术。常用的签名算法有RSA算法和DSA算法等。
- 访问控制机制：访问控制机制对应访问控制服务。通过预先设定的规则对用户所访问的数据进行限制。通常，首先是通过用户的用户名和口令进行验证，其次是通过用户角色、用户组等规则进行验证，最后用户才能访问相应的限制资源。一般的应用常使用基于用户角色的访问控制方式，如RBAC（Role Basic Access Control，基于用户角色的访问控制）。
- 数据完整性机制：数据完整性机制对应数据完整性服务。数据完整性的作用是为了避免数据在传输过程中受到干扰，同时防止数据在传输过程中被篡改，以提高数据传输完整性。通常可以使用单向加密算法对数据加密，生成唯一验证码，用以校验数据完整性。常用的加密算法有MD5算法和SHA算法等。
- 认证机制：认证机制对应认证（鉴别）服务。认证的目的在于验证接收方所接收到的数据是否来源于所期望的发送方，通常可使用数字签名来进行认证。常用算法有RSA算法和DSA算法等。
- 业务流填充机制：又称传输流填充机制。业务流填充机制对应数据保密性服务。业务流填充机制通过在数据传输过程中传送随机数的方式，混淆真实的数据，加大数据破解的难度，提高数据的保密性。
- 路由控制机制：路由控制机制对应访问控制服务。路由控制机制为数据发送方选择安全网络通信路径，避免发送方使用不安全路径发送数据，提高数据的安全性。
- 公证机制：公证机制对应抗否认性服务。公证机制的作用在于解决收发双方的纠纷问题，确保两方利益不受损害。类似于现实生活中，合同双方签署合同的同时，需要将合同的第三份交由第三方公证机构进行公证。

安全机制对安全服务做了详尽的补充，针对各种服务选择相应的安全机制可以有效地提高应用安全性。随着技术的不断发展，各项安全机制相关的技术不断提高，尤其是结合加密理论之后，应用的安全性得到了显著提高。本书的后续章节将以加密理论及其相应实现为基础，逐步阐述如何通过加密技术确保企业应用的安全。

1.2.3 TCP/IP安全体系结构

OSI参考模型为解决网络问题提供了行之有效的方法，但是卫星和无线网络的出现，使得现有的协议在与卫星和无线网络互联时出现了问题，由此产生了TCP/IP参考模型。TCP/IP从字面上看是两个Internet上的网络协议（TCP是传输控制协议，IP是网际协议），但实际上TCP/IP是一组网络协议，通常包括TCP、IP、UDP、ICMP、RIP、TELNET、FTP、SMTP、ARP、TFTP等协议。TCP/IP参考模型由下至上分为网络接口层、网络层、传输层和应用层。

OSI参考模型和TCP/IP参考模型的对比如图1-3所示。

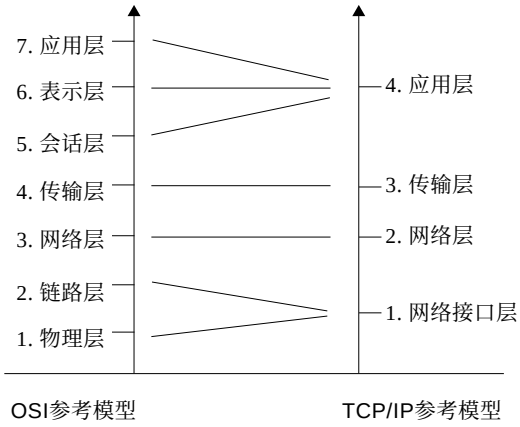

图1-3 OSI参考模型和TCP/IP参考模型对比

OSI参考模型中的物理层和链路层对应TCP/IP参考模型中的网络接口层，网络层和传输层分别对应TCP/IP参考模型中的网络层和传输层，会话层、表示层和应用层对应TCP/IP参考模型中的应用层。

对应TCP/IP参考模型，TCP/IP安全体系结构如图1-4所示。

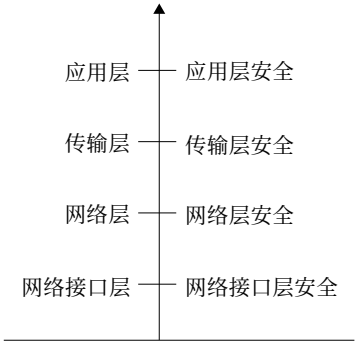

图1-4 TCP/IP安全体系结构

TCP/IP安全体系结构包括网络接口层安全、网络层安全、传输层安全和应用层安全。

- 网络接口层安全：通常指的是链路层的安全，可以通过加密方式确保数据不被窃听，通常依靠物理层加密实现。一般在通信的链路两端架设加密机，对传输的电器符号进行位流加密。
- 网络层安全：网络层的功能是负责数据包的路由选择，网络层安全就是要确保数据包能顺利到达指定的目的地。一般通过路由器硬件提高相应的安全性。
- 传输层安全：传输层的功能是解决端到端的数据传输问题。传输层提供TCP与UDP两种服务，其中TCP是可靠的、面向连接的服务；UDP是无链接的数据包服务。确保传输层安全有相应的协议，如SSL（Security Socket Layer，安全套接层协议）和TLS（Transport Layer Security，传输层安全协议）。SSL是网景（Netscape）公司设计的主要用于Web的安全传输协议，由IETF（The Internet Engineering Task Force, 互联网工程任务组，详见http://www.ietf.org/）将其标准化，进而产生了TLS，TLS是SSL的继任者。SSL 3.0与TLS 1.0差别不大，两种规范大致相同。SSL/TLS协议依赖于加密算法，使用SSL/TLS协议可使通信过程极难被窃听，保证了通信过程有较高的安全性。因此，SSL/TLS协议成为网络上最常用的安全保密通信协议，众多电子邮件、网银、电子商务、网上传真都通过SSL/TLS协议确保数据传输安全。随着卫星和无线网络的发展，WAP安全逐渐得到重视。受限于手机及手持设备的处理和存储能力，WAP论坛（http://www.wapforum.org/）在TLS的基础上进行了简化，制定了WTLS协议（Wireless Transport Layer Security，无线传输层安全）。
- 应用层安全：应用层是与应用结合最紧密的一层，负责与应用交互，以实现不同系统的应用之间的相互通信，完成各种业务处理、提供相应服务。为确保应用层的安全，可在应用层建立相应的安全机制，HTTPS协议的应用就是其中的一种。HTTPS（Hypertext Transfer Protocol over Secure Socket Layer）协议是Web上最为常用的安全访问协议，简

单地说就是HTTP安全版，从HTTPS全称不难看出它是基于SSL/TLS的HTTP协议，或者说是HTTPS=SSL/TLS+HTTP。同时，得益于SSL/TLS的高度安全性，HTTPS广泛应用于互联网上的敏感数据交互，例如B2C、网上银行、企业应用之间的数据传递等。本书将在后续章节讲解如何通过HTTPS确保企业应用的安全。

TCP/IP安全体系中，网络接口层安全、网络层安全部分主要通过相应的硬件设施来完成，传输层安全和应用层安全通过HTTPS协议以软件方式完成。

1.3 捍卫企业应用安全的银弹

通过对1.2节的学习，我们已经找到了处理安全问题的武器。但是，我们还缺少一枚解决安全问题的银弹——密码学。的确，密码学是企业应用安全问题领域的一枚银弹，是解决安全问题的核心所在。

1.3.1 密码学在安全领域中的身影

安全领域离不开密码学的支持。例如，在OSI安全体系结构中通过数据加密确保数据的保密性，在TCP/IP安全体系结构中以加密算法为基础构建SSL/TLS协议，这些都说明密码学与安全问题密不可分。

密码学在加密算法上大体可分为单向加密算法、对称加密算法、非对称加密算法三大类。MD5、SHA算法是单向加密算法的代表，单向加密算法是数据完整性验证的常用算法。DES算法是对称加密算法的典型代表，对称加密算法是数据存储加密的常用算法。RSA算法是非对称加密算法的典型代表，非对称加密算法是数据传输加密的常用算法。对称加密算法也可以用做数据传输加密，但非对称加密算法在密钥管理方面更有优势。相对对称加密算法而言，非对称加密算法在安全级别上等级更高，但非对称加密算法在时间效率上远不如对称加密算法。

以密码学为基础的各种安全实现相继出现，如HTTPS协议和一系列的“数字技术”（数字摘要、数字信封、数字签名、数字证书等），这些构成了认证技术的基础。

密码学为安全领域筑起了一道铜墙铁壁。

1.3.2 密码学与Java EE

Java EE对密码学的支持是相当广泛的，主要表现在如下几个方面：

- Java API支持：Java API支持多种加密算法。如MessageDigest类，可以构建MD5、SHA两种加密算法；Mac类可以构建HMAC加密算法；Cipher类可以构建多种加密算法，如DES、AES、Blowfish对称加密算法，以及RSA、DSA、DH等多种非对称加密算法；Signature类可以用于数字签名和签名验证；Certificate类可用于操作证书；等等。
- JSP容器支持：常用的应用服务器（如Tomcat）通过简单的配置即可支持SSL/TLS协议，获取证书配置，有效地构建HTTPS应用。

- Java工具支持：通过KeyTool可以很好地完成密钥管理、证书管理等；通过JarSigner可以完成代码签名。

1.4 为你的企业应用上把锁

终于，我们准备好了应对企业应用安全问题的良策。现在，让我们为自己的企业应用装上这一道道的安全锁。

- 访问控制：通过为用户设定用户名和口令控制用户访问权限。这是我们最常用的，也是最简单的防范措施。随着企业应用业务的不断细化，如何划分用户访问控制权限，如何控制不同类型的用户（如超级管理员、普通用户、VIP用户）访问受限资源成为新的问题。通常依靠各种理论基础来划分，比较常用的划分方式有，如以用户组为单位划分某组用户可以访问某些资源（Linux操作系统是这种划分方式的典型代表）；以用户角色为单位划分具有何种角色的用户可以访问哪些相应的资源，如我们已经提到过的RBAC。访问控制通常没有固定的算法，由架构师根据系统设计需求进行相应的设计。访问控制仅仅能起到企业应用第一层屏障的作用，最易实现也最不安全，适用于安全系数较低的企业应用。
- 数据加密：通过对数据的加密、解密可以有效地提高企业应用的安全性。数据加密可以应用在企业应用中的多个环节。例如，可对机要数据进行加密后再存储，对用户的口令加密后存储可有效避免口令盗取导致的用户利益侵犯问题；对网络传数据加密，对用户聊天信息加密传输可以确保用户隐私不易被破译；对要传输的数据做加密摘要，各种通过网络传播的光盘文件（ISO文件）同时附有摘要信息作为验证，可以验证数据完整性。数据加密适用于多种企业应用，架构师可根据具体要求实施相应的加密防范措施。
- 证书认证：通过数字证书认证可以鉴别用户身份、消息来源的可靠性，加上HTTPS协议的支持可达到高度的数据安全性。数字证书由权威的数字证书认证中心（Certificate Authority，CA)颁布。数字证书经认证中心签名处理，任何第三方都无法修改证书的内容。数字证书自身带有公钥信息，可以对数据进行加密、解密和数字签名验证。同时，带有MD5、SHA的消息摘要信息可做自身有效性验证。数字证书鉴于自身高度的安全性通常以文件形式存储，可通过网络、物理存储载体发送给用户使用。通过读取数字证书信息，HTTPS协议得以发挥安全信道通信的作用，确保数据交互的安全性。当然，安全总是有代价的。通过数字证书对数据做处理后，网络交互时间会相应延迟，这主要是因为非对称加密算法的时间效应。但为了更高的安全性，牺牲系统响应时间是有必要的。通常在电子商务中，使用数字证书是最好的选择，也是确保安全交易的唯一选择。大型企业应用之间的大批量机要数据的交互，通常采用数字证书认证的方式。架构师可根据企业应用所处的相应领域，及不同的业务需求选择有效的数字证书确保企业应用的安全证书认证多适用于电子商务。

1.5 小结

大家都知道安全问题很重要，却不能很好地处理它。每当安全事故发生后，我们才想起要亡羊补牢，但往往为时已晚。在对安全现状做了一些简要总结后，我们发现身边的安全隐患无处不在，PDA里存的年度报表、好友的聊天信息、网上交易的银行卡号以及轻易以明文存储的口令信息等，都可能被盗取、泄露和篡改。

通过安全技术目标的定义，我们知道安全技术目标包含保密性、完整性、可用性、可靠性和抗否认性。这五项技术目标基本上概括了我们所遇到的安全隐患问题，那么我们是否有一整套可行的对策呢？安全体系结构对这个问题给予了相当权威的理论支撑。

OSI参考模型在原有网络通信七层结构的基础上构建了OSI安全体系结构，它由五类安全服务和八类安全机制构成。其中，五类安全服务以安全技术目标为主旨，包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务；八类安全机制针对五类安全服务做了详尽的补充，包括加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制和公证机制。

随着卫星和无线网络的出现，原有OSI参考模式已不能应对这些网络的安全问题，此时TCP/IP出现了，但是安全问题也随即突出。为了解决这些安全问题，TCP/IP安全体系结构诞生了，包括网络接口层安全、网络层安全、传输层安全和应用层安全四项内容。其中，网络接口层安全和网络层安全依靠物理硬件来完成，传输层安全和应用层安全通过SSL/TLS+HTTP协议（也就是HTTPS协议）来完成。

通过密码学，我们找到了应对企业应用安全问题的银弹，在Java EE企业应用中也找到了相应的支持。

虽然通过用户名和口令的方式来控制用户访问是最简单，甚至是最简陋的方法，但它仍是企业安全应用的第一道屏障。我们可以合理使用相应的访问控制理论来提高对用户访问控制的安全性。例如基于用户组与用户角色的访问控制方式。在密码学的支持下，我们可以对数据进行加密和解密，确保数据的保密性，也可以通过信息摘要的方式对数据完整性进行验证。单向加密算法可以对数据完整性进行验证，常用算法如MD5、SHA。对称加密算法可以用于数据加密存储，常用算法如DES。非对称加密算法可用于数据加密传输，常用算法如RSA。我们制定出了相应的算法，同时也需要相应的载体。数字证书作为一种凭证、一种载体，可以用于数字加密解密、数字签名验证、自身有效性验证，尤其是当数字证书结合HTTPS协议应用于电子商务后，极大地提高了网络通信的安全性。

随着计算机技术的不断发展，新的存储方式、新的网络结构将层出不穷，相应的商务应用环节也会发生翻天覆地的变化，紧随其后的安全问题也会“穷追不舍”。虽然我们可以通过各种技术相应提高企业应用的安全性，但这些技术统统基于密码学理论。同样，密码学并不是固若金汤般的坚不可摧，密码学的破解每一天都有发生。我们应当合理使用各种安全技术，使其有机结合、优势互补，确保企业应用具有更高的安全性。