안전한 e-비즈니스 구축

JTC1/SC27/WG1(보안기술-보안 서비스 및 가이드라인) 컨비너 Prof. Edward (Ted) Humphreys 기고

기계건설표준팀
02-509-7290

IT 보안분야 개척자인 영국 캠브리지대학의 Roger Needham에 따르면, "IT 보안은 사용자에게 더욱 더 큰 문제로 부각되고 있다."고 한다. 내부사용자와 외부사용자로 인한 비즈니스의 위험요소가 증가하면서 많은 기업들이 이 메시지가 의미하는 바를 점점 더 인식하게 되었다. 이용자와 온라인 비즈니스와 관련한 많은 정보보안 위험이 오늘날 비즈니스 세계에 영향을 미치고 있다. 예를 들면, 부정거래, 위조문서, 소비자 상세정보, 금융· 신용카드 세부정보 유출, 피싱(금융기관이나 유명 전자상거래 업체를 사칭하여 금융정보를 빼냄) 등이 있다.

안전하게 e-비즈니스 거래를 지원하기 위해 JTC1/SC27(보안기술)에서 제정한 몇 개의 국제표준을 알아보려고 한다. 이는 암호화 정보에 대한 암호법과 프로토콜을 기반으로 한 표준들로서 암호화 정보처리 시에 사용되는 정보를 디지털 방식으로 승인하고 처리단계에서 관련 사용자들을 식별하고 인증한다.

안전한 비즈니스

암호법과 기술은 다른 곳에서도 적용될 수 있다. 예를 들어, 전자문서, 온라인 거래 또는 기타 정보의 e-비즈니스 교환 시에 보증하고 보호하는 역할을 하거나, 전자문서 발신자가 문서 발신을 부인하지 못하도록 하거나, 통신집단에 신분을 입증할 때도 이용된다. 이들을 보안서비스라고 e-비즈니스에서는 말한다.

IT 보안 표준기술의 조항이 상당히 요해져서, 최근 몇 년 동안 특히 e-비즈니스 관련 한 광범위한 암호기술에 대한 표준을 제정했다. 여기서는 기본적인 요구사항 즉 암호, 신분· 인증, 디지털 서명에 초점을 맞췄다.

사용자 인증과 기기

온라인 비즈니스상에 포함된 두 개 또는 그 이상의 집단 간에 안전한 커뮤니케이션이 이루어지기 위해서는 인증기법과 관련 기술을 알맞게 사용해야 한다. 온라인 처리, 모바일 커뮤니케이션, e-계약, 환, e-영수증 또는 기타 e-문서와 같은 많은 비즈니스상에서 어떤 형식으로든 신분인증과정이 필요하다.

인증과정에는 다양하고 복잡한 기법이 사용된다. 보안통제의 기본 형식으로는 사용자의 비밀번호 또

는 개인식별번호(PIN)를 기반으로한다. 보다강력한 형식은카드또는토큰장비로사용자들에게알려진 정보를조합하는 보안방식으로사용할수 있다. 이러한진보된조합보안기법으로지문, 음성인식, 홍채스캐너와같은생체정보도사용할 있다.

인증 표준

ISO/IEC 9798(정보기술-보안기술-실체인증)은 6부로 구성되어있고, 사용자또는 기기를확증할수 있는메커니즘을기술하고있다. 실체(예, 사용자, 컴퓨터, 통신기기)는신분을입증하기위해비밀정보를 증명해야한다.

집단간에교환하는개별메시지암호기법을사용하여보호된다. 그러나성공적으로인증하기위해서는많은암호알고리즘은암호문을본래의문자열로바악의있는어떤집단이사용자로가장하여오래된메시꾸는해독과정을제공하기위해요하다.
지를단순반복하여발송하는것을막기위해메시지의 적시성(timeliness) 입증해야한다. 그래메시지의 신선함을살리기위해 타임스탬프또는임의시도(random challenge)와응답과같은기술활목시켰다.

ISO 9798의 1부는일반적인사항이고이와는별도로 2부에서6부까지는디지털서명, 암호, 메시지인증코드와같이각기다른형식의암호기술들을기반으로한 메커니즘을구체화하고있다. 서명관련표준들은e-비즈니스와특히관련이있어서후반후에다시언급될것이다.

e-비즈니스 처리의 비밀성 보호

암호기술의중요한목적은저장된데이터나전송한 데이터의비밀성을보호하는것이다. 즉인증되지 않은사용자가읽어볼수 없도록데이터를숨기는것이다. 이러한기술은신용카드상세사항과온라인은행업무, 쇼핑관련 금융정보, 기타전자 형식으로민감한정보를보호하는데사용한다.

암호 표준

암호화는키를가진사람이외에는읽지못하게하기위해알고리즘을이용한정보처리의과정이다.

ISO/IEC 18033(정보기술-보안기술-암호알고리즘)은 총 4부로구성되어있고블록암호, 스트림암호와 같이각기다른형식의알고리즘을기술하고있다.

암호알고리즘은암호문(ciphertext) 또는암호화된 데이터의본래의문자열(plaintext)에 대한정보를알려주지않도록구성되어있다. 예를들어온라인상에 보내진신용카드상세정보는코드화되어숨겨진다. 많은암호알고리즘은암호문을본래의문자열로바꾸는해독과정을제공하기위해요하다.

디지털 서명 비즈니스

전자디지털서명은문서에직접 서명하는것과같은 목적으로이용된다. 이는서명자를인증하고서명한정보를보존하기위해사용되옌다.

디지털서명은전자지불, 웹브라우저를통한정보교환, 세금기록과관련된건강관리시스템의환자의 기록, 기타법적문서, 온라인쇼핑, 신용카드처리에 이용되고있다.

디지털서명은핸드폰, 모바일컴퓨팅기기, 스마트카드, 기타IC(integrated circuit) 카드, 웹브라우저등에 포함되면서몇개의디지털서명안이표준화되었다. 이 표준은적용과기술변화와제약을고려하여광범위한 이행옵션을제공하고있다. 예를들면명이필요한 메시지· 문서범위· 크기, 보전및 전송제약· 용량, 서명속도, 검증및성능과관련된것을제공한다.

디지털 서명 비즈니스

ISO/IEC 9796(정보기술-보안기술-메세지복원형디지털서명기법)은총 3부로구성되어있으며저장공간과 전송 부담(overhead)을 줄이기위해 부분적또는 전체메시지복원할수 있는디지털서명메커니즘에대한규격이다.

이규격의2부에서는메시지복원을실현하는세가지 전자서명스키마를규정한다. 3부에서는메시지복원형의두 가지랜덤화된디지털서명기법을기술하고있다.

이 표준안들은서명을사용할시에 데이터부담(overhead)을 최소화시키기위해구체적으로구성되어 있어저장공간이나커뮤니케이션대역폭이아주 제한이되어있는제약된환경에서적용될수 있다. 예를 들어, 잠재적인적용영역으로스마트카드와개인용휴대기기들이포함된다.

ISO/IEC 14888(정보기술-보안정보-부가형디지털서명)은검증키들의분산화와관련하여두 가지형식의 디지털서명메커니즘에대해 기술하고있다. (1) 검증키가서명자신분을공용 기능으로할 경우에는 신분기반의메커니즘이고(2)검증키로서명자의신분을확인할수 없을경우는인증서를기반으로한메커니즘이다.

ISO/IEC 14888은다음을포함하여총3부로구성된다.

- 서명을기재하고디지털서명의검증과정에대해 기술한일반모델
- 서명자의서명으로서명자의신분을확인하는신분기반메커니즘
- 인증서기반의메커니즘

요약하면ISO/IEC 14888은 일반적으로적용할수 있는서명메커니즘을제공한다.

이러한시점에서ISO/IEC 10118(정보기술-보안기술-해시함수) 규격을얻급할필요가있다. 이규격은 4부로구성되어있으며암호해시함수에대한규격이다. 해시함수는데이터를보다작은숫자로바꾸는 방법이다. 알고리즘은이렇게만들어진데이터를잘라서섞는다.

이러한해시함수는ISO/IEC 9796과 ISO/IEC 14888를포함하여거의모든실용디지털서명안에들어가 있다. 그러므로서명안사용자는해시함수를선택해야 한다. ISO/IEC 10118에서는광범위한해시함수를 제공하여다양한컴퓨터기법을사용하고있다.

ISO/IEC 15946(정보기술-보안기술-타원형곡선에기반의암호기술)은총 4부로구성되어있고타원형곡선의대수구조를기반으로다른종류의기법을또한기술하고있다.

미래

이 글을통해안전한e-비즈니스구축을위해사용되는몇개의국제표준을설명하였다. 이규격들은온라인비즈니스를이용하는기업에게도움이된다.

미래에는개발될영역중의하나는비즈니스상의 관리(management)와 관련된영역이다. 이영역의표준들이내년에발간될것으로예상된다. 이러한표준들은확인되지않은사용자가민감하고중요한비즈니스정보에접근하는것을막는데중요한역할을할 것이다. 다른중요한영역으로는현재식별및 인증툴박스에추가로생체표준을개발하는것이다.