

FNS

(Fundamental Network Security)

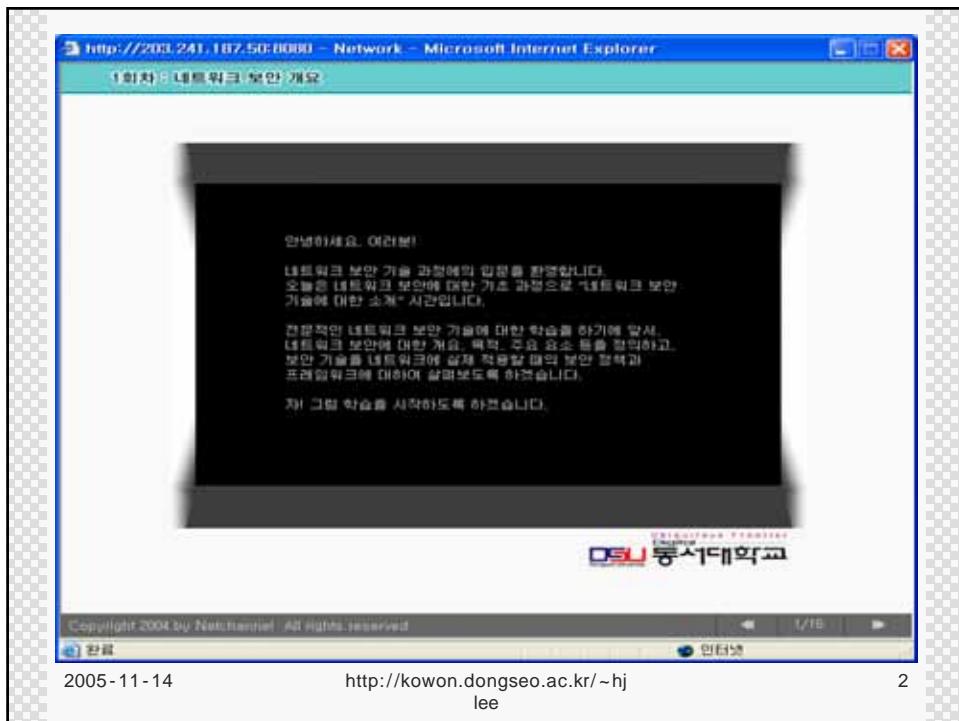
Ch1.

hjlee@dongseo.ac.kr
<http://kowon.dongseo.ac.kr/~hjlee>
<http://crypto.dongseo.ac.kr>

2005-11-14

[http://kowon.dongseo.ac.kr/~hj
lee](http://kowon.dongseo.ac.kr/~hjlee)

1



2005-11-14

[http://kowon.dongseo.ac.kr/~hj
lee](http://kowon.dongseo.ac.kr/~hj
lee)

2

1회차 네트워크 보안 개요

이번 강의의 학습목표를 살펴 봅시다.

학습 목표

- 네트워크 보안의 개념과 필요성을 설명할 수 있다.
- 네트워크 보안의 주요 목적 세 가지를 설명할 수 있다.
- 네트워크 보안의 주요 요소 다섯 가지를 설명할 수 있다.
- 네트워크 보안 정책과 네트워크 보안 프레임워크의 개념을 설명할 수 있다.

2/16

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 3

1회차 네트워크 보안 개요

먼저, 네트워크 보안이 무엇인지부터 알아 봅시다.

네트워크 보안이란?

오직 특정 사용자에게만 네트워크 자원에의 접속과 이용을 허용하는 것
특정 사용자는 별도의 보안 접속 기능이나 자원 접속 설정 과정을 통해서
네트워크 자원을 이용할 수 있음

Closed Network:
Remote Site → Frame Relay → DS Leased Line

Mobile and remote users:
Internet-based Internet(VPN) → Internet-based extranet(VPN)

Remote site:
PSTN → Internet

Partnet site:
PSTN → Internet-based extranet(VPN)

3/16

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 4

1회차 : 네트워크 보안 개요

네트워크 보안 개요

네트워크 보안의 필요성

인터넷에 연결된 모든 네트워크 사용자는 인터넷 기술 자체의 특성과 다음과 같은 여러 가지 상황 때문에 항상 네트워크 보안에 대한 위협을 받고 있다.

- 네트워크 공격의 증가
- 네트워크 공격 기술의 고도화
- 네트워크 서비스에의 의존도 증가
- 조란민 간문 보안 기술자의 부족
- 네트워크 공격에 대한 이해 부족
- 네트워크 보안 정책의 부재
- 네트워크 자원에의 무분별 접근
- 네트워크 보안 관리 체계 미비

네트워크 보안이란?

간접한 여러 가지 네트워크 보안에 대한 위협으로부터 네트워크 자원에 보안 기능을 제공하는 것은 개인의 재산을 보호하는 것과 동일한 개념이다. 어느 누가 자신의 재산과 자신이 자신도 모르는 제 3자에 의해 도용되는 것을 원하지는 않다.

결국, 네트워크 보안은 외부인에 의한 악의적인 공격에 대한 네트워크 자원 보호를 의미하며, 구체적으로 다음과 같은 요구 사항을 포함한다.

- 권한을 부여 받은 사용자만이 특정 작업을 수행 할 수 있어야 한다.
- 사용자 별로 자신이 권한을 부여 받은 정보만을 이용할 수 있어야 한다.
- 일반 사용자가 중요한 시스템의 데이터와 애플리케이션의 운용 환경에 변경을 거하거나 손상을 입힐 수 있에서는 안된다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 5

1회차 : 네트워크 보안 개요

네트워크 보안의 목적

기밀성 (Confidentiality)

기밀성의 정의

네트워크 보안에서 기밀성이란 인기되지 않은 제 3자로부터 데이터를 보호하는 것이다.

기밀성이 보장되어야 할 데이터에는 어떤 것이 있을까?

인터넷을 이용한 비즈니스 분야에서 보호해야 할 데이터는 회사 대부분의 데이터뿐만 아니라 고객의 신상정보를 포함한 고객의 인터넷을 이용한 모든 다양한 활동 정보를 대상으로 한다.

기밀성 제공의 필요성

기밀성은 다시 말해서 인터넷 상의 중요한 데이터에 프라이버시 (privacy)를 보호하는 것이다. 개인적 사생활에 프라이버시가 필요하듯, 네트워크 자원에 제작되어 있거나 네트워크 자원 상에서 견조되는 거의 모든 데이터는 기밀성이 보장되어야 한다.

비즈니스 분야에서의 기밀성 제공 범위와 제공 방안

회사나 기관의 데이터는 기본적으로 기밀성이 보장되어야 한다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 6

1회차 : 네트워크 보안 개요

네트워크 보안의 목적

무결성 (Integrity)

무결성의 정의

- 네트워크 보안에서 무결성이란 원래의 데이터가 인터넷 상에서 전송되는 도중에 인증한 사용자가 아닌 제 3자에 의해 변경되거나 파괴되지 않도록 하는 것이다.

데이터의 무결성을 어떻게 확인할 수 있을까?

- 데이터의 무결성 확인을 간단하게 설명하면 전송한 데이터의 내용과 수신된 데이터의 내용이 일치하는지 안 하는지 확인하는 것이다.

무결성 제공의 필요성

예를 들어, 인터넷 맹점을 생각해보자. 친구의 은행 계좌로 송금을 하는데, 송금 암호를 수정하기 위한 정보 중 수취인 계좌가 도중에 변경되거나 송금 금액이 제 3자에 의해 변경된다면 이는 예전 갑작한 문제가 아닐 수 없다.

비즈니스 분야에서의 무결성 제공 범위와 제공 방안

- 전송되는 모든 데이터는 기본적으로 무결성이 보장되어야 한다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 7

1회차 : 네트워크 보안 개요

네트워크 보안의 목적

가용성 (Availability)

가용성의 정의

- 네트워크 보안에서 가용성이란 컴퓨팅 시스템이 연속적으로 또한 정상적으로 동작해야 한다는 것이다.

가용성 개발

- 인터넷 상의 애플리케이션은 애플리케이션 별로 서로 다른 가용성 개발을 가지고 있다. 어떤 서비스는 면밀히 살피면 서비스를 제공하기도 하지만 어떤 서비스는 특정 날짜 및 시간에는 관리 차원에서 서비스를 중지하기도 한다.

가용성 제공의 필요성

인터넷 사용자는 언제든 원하는 시간에 원하는 정보를 얻고자 한다. 그러나 원하는 정보를 저장하고 있는 컴퓨팅 시스템이 일의의 공격을 받아 정상적인 서비스를 할 수 없거나 이에 해당 시스템에 접속할 수 없는 상황. 이라면 서비스 제공 자체가 불가한 것이다.

비즈니스 분야에서의 가용성 제공 범위와 가용성 제공 방안

- 인터넷 상의 애플리케이션을 비롯하여 데이터베이스 서버, 스토리지 장치, 네트워킹 장치는 모든 기본적으로 가용성이 보장되어야 한다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 8

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

1회차 : 네트워크 보안 개요

- 네트워크 보안의 주요 요소**
 - 네트워크 사용자를 포함하여 네트워크 상의 호스트, 애플리케이션 서비스, 그리고 각종 네트워크 자원을 통제하고 명확하게 식별하는 것이다.
 - 사용자 식별을 하는 표준 기호로는 사용자 ID와 암호와 같은 간단한 방법에서 사용자 인증과 권한 부여 및 자원 이용 현황까지 종합적으로 제공하는 고급 기술에까지 다양한 방법이 있다.
- 네트워크 경계 보안 (Perimeter Privacy)**
 - 인가된 사용자와 정보만이 보안 네트워크를 통과할 수 있도록 하기 위하여 중요한 네트워크 자원에의 접속을 제어하는 것이다.
 - 방화벽 (Firewall)이나 패킷 필터링을 하는 리우터, 스위치가 이에 해당한다.
- 데이터 프라이버시 (Data Privacy)**
 - 제 3자에 대한 정보 도청을 막기 위하여 인증된 파일 통신을 제공하는 것이다.
 - 인터넷 속에서 정보 도청을 막기 위하여 터널링 기술을 주로 사용한다.
- 보안 모니터링 (Security Monitoring)**
 - 네트워크 보안 기능들을 규칙으로 감시하고 점검하는 것이다.
 - 네트워크 휴대폰 스파너, 험프터지 시스템과 같은 도구를 이용한다.
- 정책 관리 (Policy Management)**
 - 정책 관리는 네트워크의 양적 성장과 복잡성 증가에 따른 각종 보안 상태의 분석, 평가, 구성, 감시를 수행하는 것이다.
 - 정책 관리 도구 중에는 표 기반의 사용자 인터페이스를 가진 것도 있다.

▶ 음악 시연

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 9

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

1회차 : 네트워크 보안 개요

- 네트워크 보안 정책과 프레임워크**
- 네트워크 보안 정책**
 - 네트워크 보안 정책의 정의**
 - 일반의 기관이 소유하고 있는 기술과 정보 자산에의 접속을 허용 받은 사용자가 준수해야 할 규칙들에 대한 정식 문서를 의미한다.
 - 네트워크 보안 정책의 필요성**
 - 협체의 보안 상황에 대한 기준을 작성할 필요가 있다.
 - 보안 기능 구현을 위한 프레임워크를 설정할 필요가 있다.
 - 인가 및 배안가 자원 사용 기준을 정의할 필요가 있다.
 - 보안 기능 구현에 필요한 도구와 절차를 결정할 필요가 있다.
 - 모든 사용자에 대한 협의 도록 및 역할을 정의해야 할 필요가 있다.
 - 보안 문제를 어떻게 처리할지를 정의해야 할 필요가 있다.
 - 보안 정책 구성 요소**


2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 10

http://203.241.187.50:8080 – Network – Microsoft Internet Explorer

1회차 : 네트워크 보안 개요

네트워크 보안 정책과 프레임워크

- 네트워크 보안 프레임워크**
 - 네트워크 보안 과정은 보안 정책을 기반으로 운영되는 연속적인 프로세스이다.
- 네트워크 보안 프레임워크**
 - 보안 바퀴 (security wheel)라고 일반적으로 불리는 보안 프레임워크는 아래와 같은 네 가지 단계를 끝없이 순환하는 구조를 가진다.

보안 (secure)

비인가 사용자의 자원 접근 및 자원 이용을 막고, 정보를 보호하기 위한 보안 솔루션을 구현하는 단계이다. 구체적으로 인증, 암호화, 방화벽, 보안 자원 탐색 방지 프로그램의 패치 등이 있다.

향상 (improve)

'감시' 및 '시험' 단계를 통해 얻은 정보를 기초로 보안 기능 구현을 향상하는 단계이다. 필요 시 보안 정책의 일부를 조정하기도 한다.

감시 (monitor)

보안 정책 위반 사례를 검출하고 제 1 단계 "보안"에서 구현된 보안 기능을 강화하는 단계이다. 실시간 침입 탐지 시스템을 주로 사용한다.

시험 (test)

시스템 검사 및 보안 기능의 취약점 스캐닝을 통하여 보안 정책의 효율성을 검증하는 단계이다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 11

http://203.241.187.50:8080 – Network – Microsoft Internet Explorer

1회차 : 네트워크 보안 개요

네트워크 보안 개요

지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.

네트워크 보안의 필요

특정의 악의적인 사용자에게만 네트워크 자원에의 접근과 이용을 허용하는 것이다.

네트워크 보안의 목적

네트워크 보안의 세 가지 주요 목적은 기밀성, 무결성, 가용성이다.
기밀성은 데이터가 비인가 사용자에게 노출되는 것을 보호하는 것이다. 무결성은 데이터가 비인가 사용자에 의해 변경 및 손상되는 것을 막는 것이다. 가용성은 컴퓨팅 시스템의 연속적인 운영으로 활약된다.

네트워크 보안의 주요 요소

네트워크 보안의 다섯 가지 주요 요소로 사용자·작업, 네트워크 경계 보안, 데이터 프라이버시, 보안 모니터링, 정책 관리가 있다.

네트워크 보안 정책과 프레임워크

임의의 기관이 소유하고 있는 기술과 정보 자산에의 접근을 허용 받은 사용자가 준수해야 할 규칙들에 대한 정식 기준을 보안 정책이라 하며, 보안 바퀴를 기반으로 보안 정책을 지속적으로 유지, 관리한다.

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 12

Fundamental of Network Security

1회차 네트워크 보안 개요

학습자 목표

1. 네트워크 보안 개념
2. 네트워크 보안의 필요
3. 네트워크 보안의 주제 및 목표
4. 네트워크 보안 정책과 프레임워크

▲/▼/정/비
◀/▶/다/지/기

Q 이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.

1. 통신 프로토콜 자체가 가지고 있는 고유의 취약점을 다음 중 어떤 내용으로 보안 취약점으로 말하는가?

(1) 구조/설정 상의 취약점
(2) 기술 상의 취약점
(3) 적용 프로토콜 자체의 취약점
(4) 보안 정책·상의 취약점

2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 13

NET CHANNEL Total Engineering Solution Provider

Fundamental of Network Security

1회차 네트워크 보안 개요

학습자 목표

1. 네트워크 보안 개념
2. 네트워크 보안의 필요
3. 네트워크 보안의 주제 및 목표
4. 네트워크 보안 정책과 프레임워크

▲/▼/정/비
◀/▶/다/지/기

Q 이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.

2. 다음 중 네트워크 보안의 세 가지 목적에 포함되지 않는 것은?

(1) 사용자 식별 (Identity)
(2) 기밀성 (Confidentiality)
(3) 무결성 (Integrity)
(4) 가용성 (Availability)

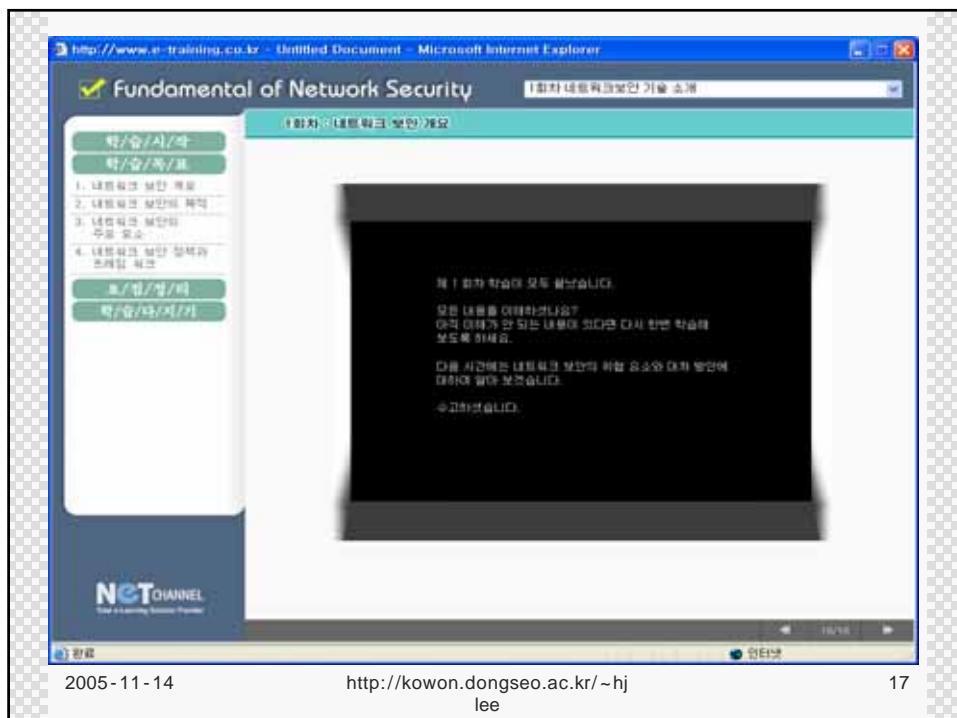
2005-11-14 http://kowon.dongseo.ac.kr/~hj lee 14

NET CHANNEL Total Engineering Solution Provider

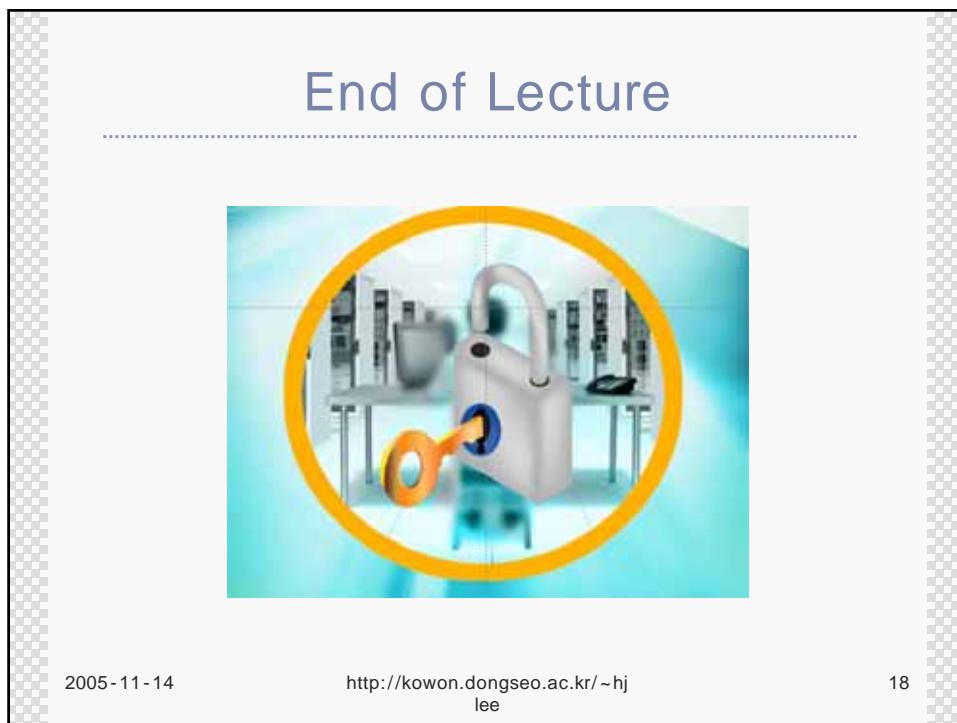
The screenshot shows a Microsoft Internet Explorer window with a slide from a network security course. The slide title is "Fundamental of Network Security". It features a red book icon and text about the four pillars of network security: Parameter security, Data privacy, Policy management, and Security management. A sidebar on the left lists course topics such as Network Fundamentals, Network Security, Network Services, and Network Management.

The screenshot shows a Microsoft Internet Explorer window with the following details:

- Title Bar:** http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
- Page Header:** Fundamental of Network Security (with a checkmark icon)
- Page Content:**
 - Left Sidebar:** Includes sections for '학습자료' (Study Materials), '교재/교과서' (Textbooks/Textbooks), '교재/교과서/교재' (Textbooks/Textbooks/Textbooks), and '교과서/교과서/교재' (Textbooks/Textbooks/Textbooks).
 - Main Content Area:**
 - Image:** A red book icon.
 - Text:** 이번 시간에 학습한 내용에 대해 정확한 이해였는지 학습율가를 통해 확인해 보도록 합니다.
 - Question:** 4. 다음 중 대화형 워크 보안 정책을 구현하는 보안 프로토콜은 (보안 방식)의 수단 단계를 통하여 나열한 것은?
 - 보안 → 서할 → 할당 → 갑지 → 보안
 - 보안 → 갑지 → 서할 → 할당 → 보안
 - 보안 → 서할 → 할당 → 갑지 → 보안
 - 보안 → 갑지 → 할당 → 서할 → 보안

A screenshot of Microsoft Internet Explorer displaying a web page titled "Fundamental of Network Security". The page content is in Korean and discusses network security concepts. It includes a large image of a padlock and a key. The browser status bar shows the URL as http://www.e-training.co.kr/Untitled Document - Microsoft Internet Explorer.

2005-11-14 http://kowon.dongseo.ac.kr/~hj
lee 17

A slide titled "End of Lecture" featuring a decorative illustration of a silver padlock with an orange key inserted into it, set against a blue background. The slide has a light gray border.

2005-11-14 http://kowon.dongseo.ac.kr/~hj
lee 18