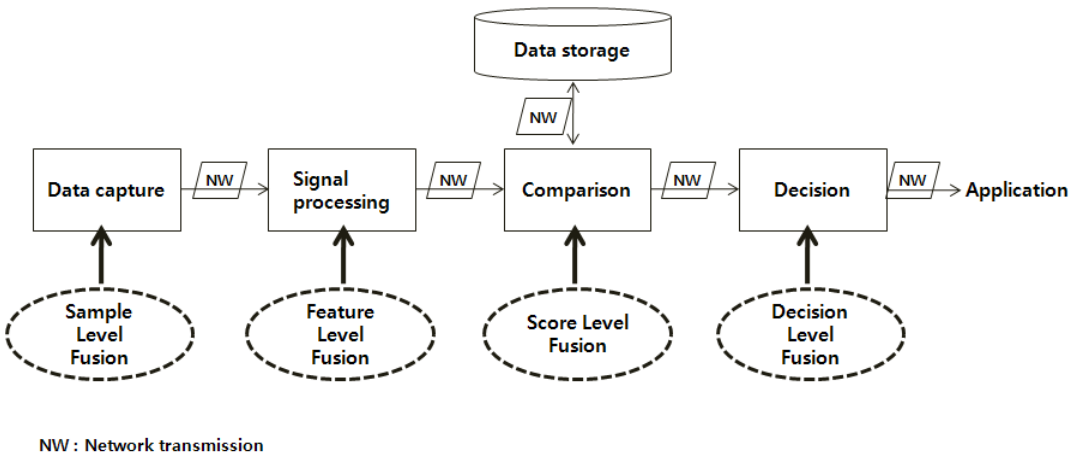
[정보보호] 멀티 바이오인식 시스템의 외부 공격과 방어

ITU-T Recommendation X.1086 Telebiometric Protection Procedure - A Guideline to Technical and Managerial Countermeasures for Biometric Data Security는 바이오인식 시스템이 운영될 때 발생하는 통신상의 공격과 방어에 대하여 기술적, 관리적 관점에서 기술하고 있다. 이때 운영되는 시스템은 단일 바이오정보를 이용하는 단일 바이오인식 시스템이다. 보안과 신뢰성의 관점에서 단일 바이오인식 시스템을 멀티 바이오인식 시스템으로의 확장이 시도되고 있다. 멀티 바이오인식 시스템은 바이오인식 시스템의 운영이 멀티 바이오정보의 사용과 바이오인식 시스템의 각 단계 상의 융합(Fusion)이 이루어지는 시스템이다.

멀티 바이오인식 시스템에서의 융합

멀티 바이오인식 시스템은 바이오인식 시스템이 원격지에서 운영될 때 시스템의 처리 단계에서 각각의 모듈들에 대한 융합(Fusion)이 발생한다. 하나의 바이오정보를 이용하는 단일 바이오인식 시스템에 비하여 2개 이상의 바이오정보를 이용하는 다중바이오인식 시스템의 경우, 바이오정보의 누출에 따른 피해가 발생할 것이다. 다중 바이오인식의 경우, 아래 그림에서 도시하는 것과 같이, 통합 모듈이 어느 위치에 존재하는가에 따라 Sample Level에서의 통합, Feature Level에서의 통합, Score Level에서의 통합, Decision Level에서의 통합으로 나눌 수 있다.



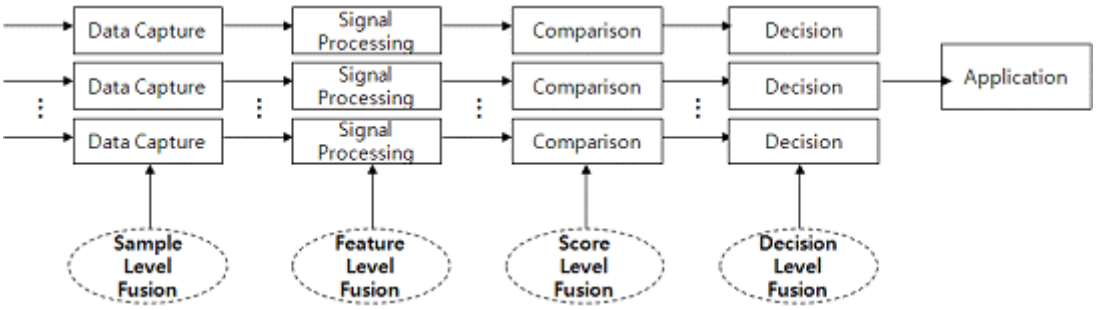
<그림 1> 멀티 바이오인식 시스템 운영 단계에서의 융합

멀티 바이오인식 시스템 융합 상의 공격과 방어

제시하는 권고사항들은 바이오인식 시스템이 통신상에서 사용될 때 발생하는 공격과 방어책에 대한 권고안(X.1086)을 수용하면서, 추가로 다중 바이오정보를 네트워크 상에서 송수신해야 하는 다중 바이오인식 시스템의 특성성을 고려한 공격과 보안대책을 제시하고 있다.

멀티바이오인식 시스템의 Sample Level Fusion에서, 모듈이 바이오인식 입력 장치로부터 다중 바이오정보를 획득하거나 원시 바이오정보의 정보의 조합으로부터 처리된 단일 바이오정보를 생성

하는 경우에 발생한다. 바이오정보의 융합은 특징 추출을 위하여 Signal processing 단계로 전송되고, 이때 처리된 결과를 바탕으로 진위여부를 결정하게 된다. 전달되는 정보가 가짜이거나 훼손된 경우에는 사용자의 진위여부 결과에 대한 신뢰성이 낮아질 것이다.



<그림 2> 멀티 바이오인식 시스템상의 공격

예를 들어, <그림 2>의 Samlple Level Fusion 단계에서의 공격은, 바이오인식 데이터가 획득되는 단말기에서 발생하는 공격으로, 불순한 의도의 사용자가 단말기를 이용하여 가짜 바이오정보를 이용하여 공격을 시도할 수 있는 것을 나타낸다. 또는 정확한 바이오정보를 전송받아 바이오정보의 특징요소를 추출하는 Signal Processing 단계에서 잘못된 특징 정보를 추출하도록 하는 공격을 받아 잘못된 특징 정보를 추출하고, 이를 전송하여 침입자의 정보가 정확한 사용자의 ID로 저장되거나 비교될 수도 있을 것이다. 이상과 같이 멀티 바이오인식 시스템의 각 모듈에서 발생 가능한 공격은 아래와 같다.

1. Sample Level Fusion:

- 공격사항
  - 악의적인 프로그램에 의해 부정확하게 융합된 데이터의 생성
  - 다른 센싱 장비를 사용하여 사용자의 바이오정보가 획득될 때, 바이오정보를 수정
  - 하나 이상의 바이오정보가 선택되었을 때 처리시간이나 복잡성이 증가
- 방어요소
  - 바이오인식 시스템에 설치된 외부 프로그램에 의하여 데이터가 조작되지 않도록 보호
  - 원시 데이터가 획득될 때 보호 절차를 제공
  - 획득장비의사용이나 비협조적인 사용자를 위하여 데이터 획득 시나리오를 구성

2. Feature Level Fusion

- 공격사항
  - 불명확한 데이터 융합이 공격자에 의하여 공격이 시도되거나, 악의적인 프로그램에 의하여 발생
  - 특징 추출 단계에서의 융합에서 불명확한 특징 집합이나 호환성이 없는 특징들 때문에 실행

하기가 어려워짐

- 방어요소
  - 교체나 수정을 예방하기 위하여, 침입자나 불법적인 공격에 대하여 보고할 수 있는 방법이 제공되어야 함
  - 융합을 하기 위하여, 융합을 위한 특징 데이터는 대응되는 공간상에 하나 이상의 데이터로 조합되도록 함

3. Score Level Fusion

- 공격사항
  - 악의적인 프로그램에 의하여 부정확하게 융합된 정합 데이터가 생성
  - 바이오정보 요소의 다른 특징들을 사용할 때, 정합 알고리즘은 이들 특징들에 따라 구분되어야 함
- 방어요소
  - 템플릿이 설치된 바이오인식 시스템이나 외부 프로그램에 의해 처리될 때 데이터 처리를 보호하기 위한 방법이 제공해야 함
  - 정합 알고리즘이 이들 정합 단계에서 특징들이 다양하게 고려될 때, 각각의 특징들이 정합되어야 하는 알고리즘이 정의되어야 함

4. Decision Level Fusion

- 공격사항
  - 조작된 비교 결과가 비교하고자 하는 모듈들로부터 획득
  - 부정확한 결과 데이터가 악의적인 프로그램에 의해 생성
- 방어요소
  - 감시하는 보호 방법들에 의하여 검사 방법 제공
  - 바이오인식 시스템에 의해 설치된 이들 예외적인 외부 프로그램에 의해 데이터의 조작을 예방하는 방법이 제공

이상과 같이 멀티바이오인식 시스템상에서 발생하는 공격과 해당 공격을 방어하고자 하는 방어요소에 대하여 ITU-T Recommendation X.1086 개정안1 (Telebiometric Protection Procedure - A Guideline to Technical and Managerial Countermeasures for Biometric Data Security : Multibiometric Protection Procedures)에서 기술하고 있다.

전인자 (와이즈오토모티브 책임연구원, ITU-T Q9 위원, injajeon@gmail.com)