프라이버시 보호 및 부인방지를 위한 물류 운송 보안 기법[1)]

최민석*, 강민수*, 이동훈*
*고려대학교 정보보호대학원
e-mail:koreacms@korea.ac.kr

Privacy protection and non-repudiation security mechanisms for logistics

Min-Seok Choi*, Dong-Hoon Lee*, Min-Soo Kang*
*Graduate School for Information Security, Korea University

요 약

개인정보보호법이 제정 및 시행됨에 따라서 고유식별정보를 처리하는 경우 그 고유식별정보가 분실, 도난, 유출, 변조 또는 훼손 되지 않아야 한다[1]. 하지만 현재 운송업계의 택배 서비스를 이용 시 고유식별정보가 고스란히 노출 되어있으며, 위·변조 또한 가능하다. 이러한 주소, 성명, 전화번호 등 개인을 식별할 수 있는 개인정보를 악용하여, 명의 도용이나 피싱 등의 심각한 문제가 발생될 수 있다. 현재 택배 시스템은 발신, 수신, 배송에 대한 사고 및 논쟁 발생 시 그에 따른 증거자료가 부족하기 때문에 책임이 불명확하다. 이를 사전에 방지하기 위해서는 관련된 증거를 생성, 수집, 유지, 활용, 검사하는 절차와 그 역할을 담당할 신뢰된 제3의 기관이 필요하다. 본 논문에서는 현재의 택배 시스템을 점검해 보고 개인정보보호 차원에서의 해결방안을 모색하는 것과 발신, 수신, 배송의 부인방지 서비스 적용을 목표로 한다.

1. 서론

개인정보보호법이 시행됨에 따라 관심과 인식이 높아지면서 개인정보를 보호하기 위해 기업뿐만 아니라 국가적으로도 많은 노력과 비용을 투자하고 있다. 하지만 대부분 온라인상에서의 개인정보보호로 오프라인에서의 개인정보보호에 대해서는 그 노력이 상대적으로 많이 부족한 현실이다. 국내의 경우 온라인에서의 개인정보 보호를 위한 법과 제도의 정비가 이뤄지고 있으나 우편, 택배 운송장으로 인한 오프라인에서의 개인정보 유출 보호방안 논의는 이루어지지 않고 있다. 국내 택배산업은 CATV 홈쇼핑과 전자상거래의 발전 등에 힘입어 날로 물량이 증가하고 있다. 운송장에는 고객의 성명과, 주소, 전화번호 등의 개인정보를 그대로 노출시키고 있으며[2], 운송장을 폐기할 때에도 각별히 신경을 써야 하는 실정이다. 실질적으로 운송장을 이용한 사회공학적 공격사례[3]와 보이스 피싱[4]이 빈번하게 발생되고 있다. 또한 현재 택배 서비스에서는 발신자의 정보가 위·변조될 수 있는 문제점을 가지고 있으며, 발신 부인방지와, 수신 부인방지, 배송 부인방지에 대한 서비스가 제공되고 있지 않으며, 그로인해 택배 서비스에서 임의배송, 수신거부, 이유 없는 배송지연 및 미배송, 물품 훼손 및 분실 등에 사고가 빈번히 발생하고 있다[5]. 이런 사고와 관련하여 논쟁이 발생 시 증거자료가 부족으로 사건을 해결하는데 많은 시간과 비용이 소요된다. 이를 사전에 방지하기 위해서는 관련된 증거를 생성, 수집, 유지, 활용, 검사 하는 절차와 그 역할을 담당할 신뢰된 제3의 기관이 필요하다. 신뢰된 제3의 기관은 발신, 수신, 배송에 대한 부인방지 서비스와 개인정보를 보호하기 위해 배송자에게 수신자의 정보를 수신자에게는 배송자의 정보를 중계해주는 역할을 담당한다.

본 논문은 운송장을 이용한 사회공학적공격을 예방하고 발신·수신·배송에 대한 부인방지 서비스와 택배 업무에서의 자동화 및 전산화를 위해서 발신자의 정보와 수신자의 정보를 코드화 및 암호화 하는 방법으로 QR-code 기반[6]의 바코드 운송장[7]과 대칭키 기반의 암호 알고리즘, 비대칭키 기반의 암호 알고리즘을 기반으로 개인정보 암호화와 부인방지 서비스를 제안한다.

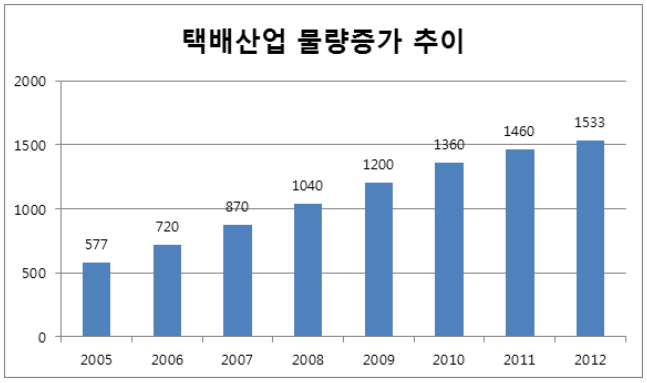
2. 기존 택배 시스템 현황과 문제점

국내 택배산업은 CATV 홈쇼핑과 전자상거래의 발전 등에 힘입어 2005년 택배물량이 5억 7천만 개에 불과하던 것이 2012년도에는 15억 3천만 개로 크게 성장하였다[7]. 하지만 물량이 많아지면서 서비스의 품질저하, 임의배송, 수신부인, 미배송, 물품 훼손 및 분실 등의 사고로 피해금액도 증가하고 있으며, 이를 해결할 수 있는 제도가 필요한 현실이다. 현재 택배피해 구제절차는 다음과 같다.

1) 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음

① 해당 택배업체와 보상협의
② 소비자상담센터 접수
③ 소비자분쟁조정위원회 조정 요청
④ 마지막으로 소비자 소송

이러한 구제절차는 복잡하고 증거자료 부족으로 시간이 오래 걸리게 된다. 이에 물류 운송 시스템에서 관련된 증거를 생성, 수집, 유지, 활용, 검사 하는 절차와 그 역할을 담당할 신뢰된 제3의 기관과 발신, 수신, 배송에 대한 부인방지가 필요한 실정이다. 또한 운송장에는 고객의 이름, 주소, 전화번호와 같은 개인을 식별할 수 있는 고유식별정보가 그대로 노출되어 있기 때문에 명의 도용이나 피싱 등의 심각한 문제가 발생될 수 있다.



(그림 1) 택배산업 물량증가 추이 (단위: 백만 개)

3. 제안하는 서비스 시나리오

2절에서 제시하였던 문제점을 해결하기 위해 본 논문에서 제안하는 서비스 요구사항과 제안 시나리오를 설명한다.

3.1 요구사항

택배 시스템에서의 부인방지 프로토콜을 적용하기 위해 요구사항은 다음과 같다.

(1) 신뢰된 제3의 기관인 TTP의 존재가 필수적이며, TTP는 서비스를 제공받는 개체(발신, 수신, 배송)의 공개키 또는 비밀키를 안전하게 공유하고 있다.

(2) 발신자는 TTP에 의해 생성된 코드와 운송장 번호를 출력 할 수 있다.

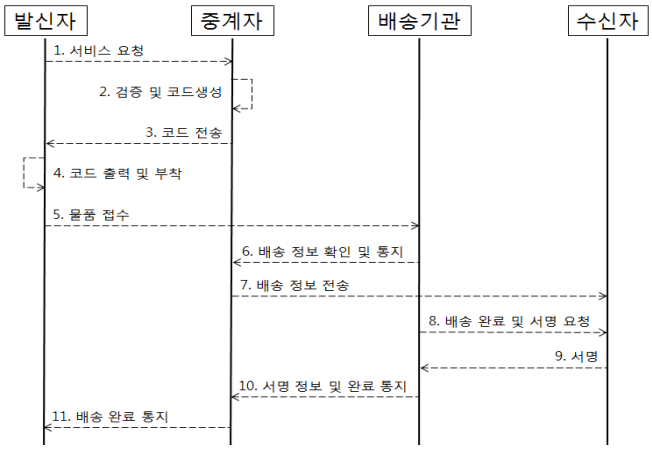
(3) 발신자는 초기 서비스 요청 시 배송기관을 선택해야 하며, 수신자는 SMS, MMS 또는 e-Mail 서비스를 제공받을 수 있다.

(4) 배송자는 QR-code를 스캔하고 TTP로 정보를 전송할 수 있는 단말기를 소지하고 있다.

(5) 서비스 제공시 생성되는 모든 정보(부인방지 토큰, 수신자 일회성 비밀키, QR-code)는 TTP에 의해서만 생성이 가능하다.

3.2 시나리오

(그림 2)는 택배 시스템에서 부인방지 서비스를 제공하기 위한 시나리오이다. 시나리오 순서는 다음과 같다.



(그림 2) 시나리오

(1) 서비스 요청 : 발신자 정보, 수신자 정보, 배송기관 코드, 배송물품 정보를 입력하고 전자서명 후 전송

(2) 검증 및 코드 생성 : 검증 단계에서 전자서명 정보 검증과 사용자가 입력한 정보 위 · 변조 검사 후 수신부인방지 토큰과 배송부인방지 토큰 생성, 코드 생성 단계에서 발신코드(수신자 일회성 비밀키로 암호화), 수신코드(배송기관 비밀키로 암호화), 운송장 번호 생성

(3) 코드 전송 : 생성된 수신코드, 발신코드, 운송장 번호 전송

(4) 코드 출력 및 부착 : 전송 받은 코드를 출력 하여 부착

(5) 물품 접수 : 사용자는 배송기관을 통해 직접 물품을 접수

(6) 배송 정보 확인 및 통지 : 배송자는 코드 리더기로 수신코드를 읽어 배송부인방지 토큰을 중계자에게 전송하고, 배송 정보를 확인 후 물품 접수 완료 통지

(7) 배송 정보 전송 : 성공적으로 물품 접수가 완료 되면 중계자는 수신자에게 발신자 정보, 물품 정보, 운송장 번호, 일회성 비밀키를 전송(SMS, MMS or e-Mail).

(8) 배송완료 및 서명 요청 : 배송자는 발신코드를 리더기를 통해 읽어 수신자에게 서명(일회성 비밀키 입력)을 요청.

(9) 서명 : 수신자는 배송자의 단말기에 서명(일회성 비밀키 입력).

(10) 서명 정보 및 완료 통지 : 배송자 단말기에서 수신자가 입력한 일회성 비밀키가 일치 하게 되면 단말기는 중계자에게 수신부인방지토큰을 전송한다.

(11) 배송 완료 통지 : 중계자는 발신자에게 배송 완료를 통지 한다.

4. 제안 프로토콜

4절에서는 프로토콜의 용어정의와 개인정보를 암호화하고 QR-code 및 부인방지 토큰을 생성하는 방법에 대한 세부적인 프로토콜을 제안한다. 부인방지는 발신 부인방지 서비스를 위한 비대칭키 기반의 부인방지[9] 기법과 수신, 배송 부인방지 서비스를 위한 대칭키 기반의 부인방지[10]

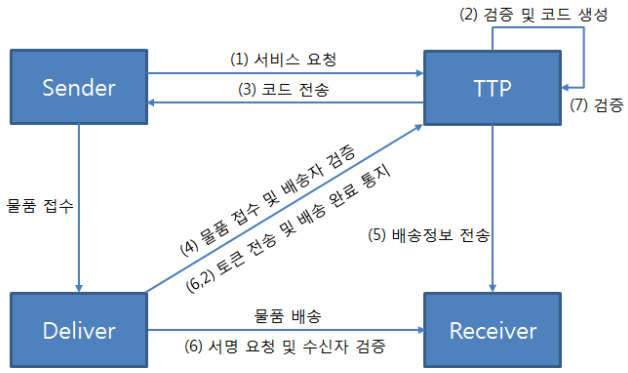
프로토콜을 제안한다.

4.1 용어정의

<표 1> 용어정의

용어	정의
TTP	신뢰된 제3의 기관(중계자), 부인방지 토큰을 생성, 발신, 수신 QR-code를 생성
MD	메시지 다이제스트(Message Digest)
S_info	발신자 정보(이름, 주소, 전화번호, etc)
R_info	수신자 정보(이름, 주소, 전화번호, etc)
D_info	배송자 정보(이름, 배송기관, 전화번호, etc)
P_info	물품 정보(발송 물품, 수량, 가격, etc)
s_key	발신자의 개인키(PKI 기반)
s'_key	발신자의 공개키(PKI 기반)
ttp_key	TTP 비밀키
d_key	배송자 또는 배송기관의 비밀키
r_key	수신자 일회성 비밀키
R_token	수신부인방지 토큰(S_info, SN, TD 정보를 ttp_key를 이용하여 MAC 생성)
D_token	배송부인방지 토큰(R_info, SN, TD를 ttp_key를 이용하여 MAC 생성)
S_code	발신 코드(P_info, SN, R_token 정보를 r_key로 암호화한 코드)
R_code	수신 코드(R_info , SN, TD, D_token 정보를 d_key로 암호화한 코드)
D_code	배송기관 코드 정보(Number or Character)
TD	서비스 요청 시간 정보 (YYYY:MM:DD:tt:mm:ssssss)
SN	운송장 번호, 증거 자료 또는 인터넷을 통한 조회 시 식별값으로 사용

4.2 암호화 기법과 부인방지 토큰과 코드 생성



(그림 3) 제안 메커니즘

(1) 서비스 요청

M = S_info || R_info || D_code || P_info

MD = HASH(M)

SD = $SIGN_{s\_key}$(MD)

M, SD TTP에 전송

(2) 검증 및 코드 생성

① 검증

M′ = S_info || R_info || D_code || P_info

MD = Hash(M′)

MD′ = $VERIFY_{s'\_key}$(SD)

MD와 MD′ 비교

② SN 생성

SN = 운송장 번호

③ Token 생성

R_token = MAC_{ttp_key}(S_info || SN || TD)

D_token = MAC_{ttp_key}(R_info || SN || TD)

④ 코드 생성

S_code = ENC_{r_key}(P_info || SN || R_token)

R_code = ENC_{d_key}(R_info || SN || TD || D_token)

(3) 코드 전송

M, S_code, R_code, SN 발신자에게 전송

(4) 물품 접수 및 배송자 검증

① 배송자 검증

R_info || SN || TD || D′_token = DEC_{d_key}(R_code)

② 배송부인방지토큰 전송 및 물품 접수 통지

D′_token, SN, D_info TTP에 전송

(5) 배송 정보 전송

S_info, r_key, SN, P_info 수신자에게 SMS, e-Mail 전송

(6) 서명 요청 및 수신자 검증

① 수신자 검증

P_info || SN || R′_token = DEC_{r_key}(S_code)

② 수신부인방지토큰 전송 및 배송 완료 통지 :

R′_token, SN TTP에 전송

(7) 토큰 검증

① 배송부인방지토큰

TTP DB에 저장 되어 있는 D_token과 배송자 단말기에서 전송 받은 D′_token 비교

② 수신부인방지토큰

TTP DB에 저장 되어 있는 R_token과 배송자 단말기에서 전송 받은 R′_token 비교

4.3 발신 부인방지

발신자는 발신자만이 가지고 있는 개인키, 그리고 TTP와 발신자간에 공유된 공개키를 가지고 있다고 가정한다. TTP는 발신자의 요청을 받게 되면 발신자에게 전자서명을 요청 하고, 발신자는 발신자의 정보와 수신자의 정보, 물품 정보, 마지막으로 배송기관을 선택 후 입력된 데이터에 발신자의 개인키로 전자서명을 하여 TTP로 전송한다. TTP는 발신자의 공개키로 전자서명을 검증한 후 운송장번호와 부인방지 토큰, QR-code를 생성하고 발신자가 보낸 정보와 생성된 정보를 저장한다. 그 후 TTP는 발신자에게 생성된 코드를 넘겨준다. TTP는 이 과정에서 발신에 대한 부인방지가 가능하며, 발신자와 수신자의 정보 또한 무결성 검증 및 보장 할 수 있다.

4.4 수신 부인방지

수신 부인방지는 TTP에서 생성한 수신자 일회성 비밀키, 발신자 정보, 운송장번호, 배송자 정보를 배송기관에서 물품 접수 완료 시점에 수신자에게 SMS, MMS, e-Mail 등으로 전송한다. 배송자가 수신자에게 물품을 배송하게 되면 배송자는 소지하고 있는 PDA 또는 스마트폰을 이용하여 발신 코드를 스캔 후 수신자에게 서명대신 TTP에서 보낸 수신자 일회성 비밀키를 요청한다. 수신자가 유효한 수신자 일회성 비밀키를 입력하게 되면 PDA 또는 스마트폰에서 수신 부인방지 토큰을 TTP에 전송하고, TTP는 기존에 저장하고 있던 수신 부인방지 토큰과 전송받은 수신 부인방지 토큰을 비교하여 검증하게 된다. TTP는 이 과정에서 수신에 대한 부인방지가 가능하다.

4.5 배송 부인방지

배송기관은 사전에 TTP와 배송기관 비밀키를 서로 안전하게 공유하고 있다고 가정한다. 발신자가 배송기관에 물품을 접수할 때 배송자는 소지하고 있는 PDA 또는 스마트폰으로 수신 코드를 스캔하게 되는데 이때 사전에 공유하고 있는 배송기관의 비밀키를 입력해야 한다. 유효한 배송기관의 비밀키를 입력하게 되면 PDA 또는 스마트폰에서 배송 부인방지 토큰을 TTP에 전송하고, TTP는 기존에 저장하고 있던 배송 부인방지 토큰과 전송받은 배송 부인방지 토큰을 비교하여 검증하게 된다. TTP는 이 과정에서 수신에 대한 부인방지가 가능하다.

5. 결론

사회적으로 큰 이슈가 되고 있는 개인정보보호는 온라인상에서는 활발히 그 연구가 진행되고 있지만 오프라인상에서의 연구는 미흡하다. 오프라인에서 우편이나 택배 운송장의 고객정보를 보호하기 위한 연구와 배송 사고 발생 시 택배회사와 고객의 충돌을 최소화하고 신속한 처리를 위해 발신, 수신, 배송에 대한 부인방지 연구가 필요하다.

본 논문은 택배 운송장에서 발신자 정보를 수신자의 일회성 비밀키로 암호화 하고 수신자 정보를 배송기관의 비밀키로 암호화하여 고객의 정보를 보호하는 방법과 부인방지 서비스를 위해 신뢰된 제3의 기관을 제안하였다. 신뢰된 제3의 기관은 부인방지 토큰을 생성하고 저장함으로써, 사고 및 분쟁 발생 시 증거자료를 활용하여 신속한 피해 처리와 보상이 가능하다.

참고문헌

[1] 개인정보 보호법, 법률 제10465호

[2] 보안뉴스 “택배업체, 고객 개인정보 보호 소홀해!” http://www.boannews.com/media/view.asp?idx=23195&kind=1, 2010. 10

[3] 이동휘, “사회공학기법을 이용한 피싱 공격 분석 및 대응기술” 정보·보안 논문지 제6권 제4호, 2006. 12

[4] 금융감독원 “보이스피싱 피해사례 발생현황”, 2011. 8.

[5] 헤럴드경제 “늘어나는 설밑 택배 관련 사고… 반갑지만은 않네요” http://biz.heraldm.com/common/Detail.jsp?newsMLId=20120120000058, 2012. 1

[6] DENSO Korea SALES CORPORATION, “QRcode manual,” in The advantage of QRcode, Ver.1007, 2010.

[7] 김석현, “개인정보를 암호화한 바코드 운송장”, 한국정보처리학회 2011. 5

[8] 물류신문 “물류시장 2011/2012 회고와 전망-택배산업” http://www.klnews.co.kr/news/articleView.html?idxno=102910, 2011. 12

[9] ISO/IEC FCD 13888-3. Infomation technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques, 2008-11-24

[10] ISO/IEC FCD 13888-2. Infomation technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques, 2009-10-19