

금융 계좌의 비상용 비밀번호를 이용한 고객상황 인지시스템

백금옥*, 임철호**

한국방송통신대학교 평생대학원 정보과학과

e-mail : whitegoldruby@hanmail.net*, point289@nate.com**

A Context-aware System of Customers with the Emergency Password of a Financial Account

Geum Ok Baik*, Cheol Ho Lim**

Dept. of Computer Science, Graduate School, Korea National Open University

요 약

가택침입이나 물리적인 납치·강도 등의 위협을 당할 경우, 개인은 외부와의 소통이 단절된 상태에서 생명의 위협과 함께 금융자산 유출의 위험에 쉽게 노출될 수밖에 없다. 본 논문에서는 이러한 상황에서 금융 계좌의 비상용 비밀번호를 이용하여 개인의 긴급한 상황을 외부에서 인지할 수 있는 고객상황 인지시스템을 제안한다. 제안하는 고객상황 인지시스템은 비밀번호 인식기, 비상상황 인식기, 경보 발령기, 비상상황 처리기로 구성된다. 제안한 시스템은 고객의 긴급 상황을 인지하여 적절히 대처할 수 있을 뿐만 아니라, 금융자산 강탈을 목적으로 하는 범죄 심리를 사전에 예방하는 효과가 있을 것으로 예상된다.

1. 서론

현대 사회는 나날이 늘고 있는 강력범죄에 따른 제3자의 강요나 협박, 납치 등으로 개인의 의지와는 무관한 금융자산의 부정출금 등 금융사고가 점차 증대되고 있는 실정이다. 특히 가택침입이나 물리적인 납치·강도 등의 위협을 당할 경우, 개인은 외부와 소통이 단절된 상태에서 생명의 위협이나 금융자산 유출의 위험에 쉽게 노출될 수밖에 없다. 물리적 상황과 위협에 개인이 무방비상태로 노출되었을 때 비고의적으로 비밀번호를 유출시킬 수밖에 없으며, 이러한 금융 사고는 개인에게 정신적·물리적 손실을 가져옴과 함께 모방범죄의 확산으로까지 파급될 수 있다.

이에 본 논문에서는 이러한 상황에서 금융 계좌의 비상용 비밀번호를 이용하여 고객이 처한 긴급한 상황을 외부에서 인지할 수 있는 고객상황 인지시스템을 제안하여 고객의 생명과 금융자산을 보호하고, 나아가 금융자산 강탈을 목적으로 하는 범죄 심리를 미연에 방지하거나 최소화시키는 데에 기여하고자 한다.

2. 상황적 범죄예방이론과 현실적 문제점

범죄행위에 있어서의 유발적 요인들을 제거하는 행위를 범죄의 유인력 제거라 하며, 이를 위한 방법으로는 타겟 하드닝(Target Hardening), 접근통제(Access Control)

등의 방법이 있다[1]. 타겟 하드닝은 방범창, CCTV 등과 같은 도구적인 방법 장치를 사용해서 범죄를 예방하는 것이다. 접근통제 방법으로는 인터넷 뱅킹의 경우를 예로 들면 공인인증서, 보안카드, 출금계좌 비밀번호, 이체 비밀번호 등이 있을 수 있다[2]. 이 외에도 범죄예방을 위한 금융전산망이 반드시 갖추어야 할 네트워크 보안방법은 기밀성, 권한(Authorization), 인증(Authentication), 무결성, 암호화, 부인부재(Non-Repudiation) 등이 있다[3].

그러나 악의적인 접근에 의한 가택침입이나 물리적인 납치·강도 등의 위협을 당할 경우 비밀번호 유출과 보안카드 또는 OTP(One-time Password)의 탈취에 의한 출금 및 이체를 막을 방법이 전무하며, 이러한 위험 상황의 통보는 고객에게 육체적·정신적·물리적 손실을 끼치고 난 후인 금융거래가 종료된 시점에서 치안기관과 금융기관에 통보되는 실정이다.

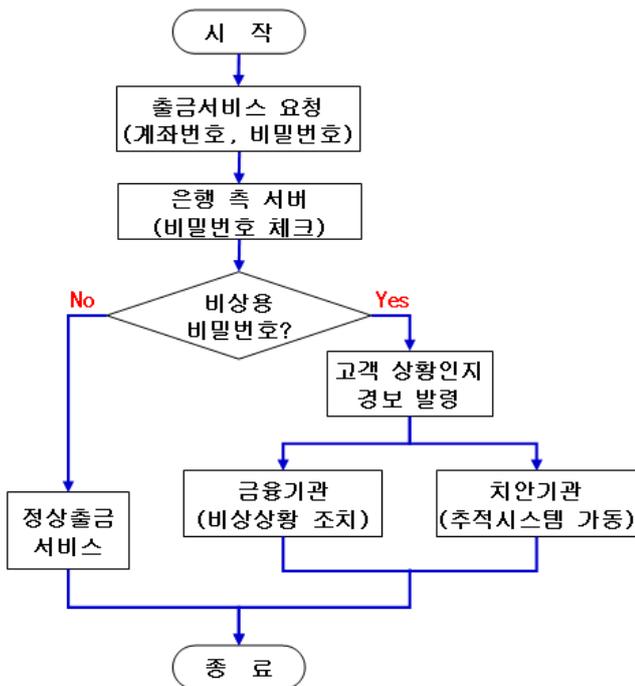
3. 제안하는 고객상황 인지시스템

3.1 시스템 개요

CD/ATM기기 거래를 비롯한 텔레뱅킹, 인터넷 뱅킹, 면대면 창구거래 등 금융기관과의 모든 거래에는 고객 계좌번호와 비밀번호를 반드시 필요로 한다. 본 논문에서 제안하는 고객상황 인지시스템은 소프트웨어적인 접근통제 방법으로서, 이러한 금융기관과의 거래에서 미리 약정된 비상용 비밀번호를 이용하여 외부로부터 완전히 고립된

고객의 위험상황을 금융기관과 외부에 알릴 수 있는 방법이다.

먼저 고객은 계좌를 개설할 때 상용과 비상용 등 용도가 서로 다른 비밀번호를 금융기관에 등록한다. 이후 고객은 외부와의 소통이 완전히 단절된 위급한 상태에서 상시적으로 사용되는 비밀번호를 대신하여, 미리 약정된 비상용 비밀번호를 범인에게 가르쳐주어 위급상황을 금융기관을 통해 외부로 알릴 수 있게 된다.



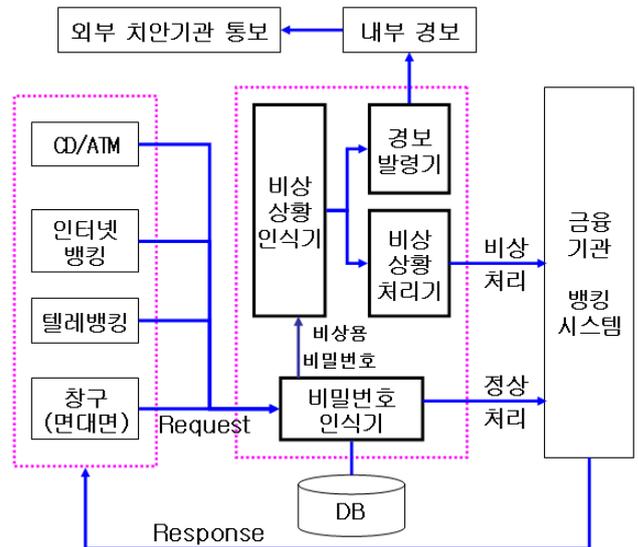
[그림 1] 고객상황 인지시스템의 처리 흐름도

[그림 1]에서와 같이 고객상황 인지시스템은 먼저 고객의 출금서비스 요청과 함께 입력받은 비밀번호가 미리 약정된 상시용 비밀번호인지 비상용 비밀번호인지를 체크하게 된다. 이때 상시용 비밀번호일 때에는 정상적인 업무 프로세스에 따라 출금 서비스가 실행된다. 만약 미리 약정된 비상용 비밀번호일 때에는 금융기관 측에 고객의 비상상황을 알리는 경보가 발령된다. 경보가 발령되면 금융기관은 치안기관에 통보함과 동시에 상대계좌의 지급정지나 계좌추적 또는 따로 정의된 매뉴얼기반(예를 들면, 창구의 지연지급이나 CD/ATM기기의 경우 통신장애/잔액부족 등 고의의 지연 메시지 발생)의 대고객 대응을 하고, 통보받은 치안기관은 추적시스템 등을 가동하여 범인을 추적 및 검거할 수 있게 된다.

3.2 시스템 구성

제안하는 고객상황 인지시스템의 구성은 [그림 2]와 같고, Banking System 앞단에 위치하여 CD/ATM기기와 인터넷 뱅킹, 텔레뱅킹, 면대면 창구 등으로부터 요청받은 서비스를 처리하게 된다. 비밀번호 인식기는 서비스 요청 시 고객으로부터 입력받은 비밀번호를 확인하여 비상용

비밀번호일 경우 그 결과를 비상상황 인식기로 넘겨준다. 비상상황 인식기는 비상조치 상황을 경보 발령기와 비상상황 처리기에 전달한다. 경보 발령기는 금융기관 내부에 비상경보가 발령되고, 내부경보가 인지되면 치안기관에 통보하고 매뉴얼기반 대응을 하게 된다. 비상상황 처리기는 예외처리를 설정하여 Banking System에 서비스를 요청한다.



[그림 2] 고객상황 인지시스템의 구성도

4. 결론

본 논문에서는 외부와의 소통이 단절된 상황에서 고객이 금융기관과의 거래에 있어 미리 약정한 비밀번호를 이용하여 외부의 도움을 요청할 수 있는 고객상황 인지시스템을 제안하였다. 제안한 고객상황 인지시스템은 고객 상황을 인지하여 고객의 생명과 금융자산을 보호할 수 있을 뿐만 아니라, 금융자산 강탈을 목적으로 하는 범죄 심리를 사전에 예방하는 효과가 있을 것으로 예상된다.

향후 연구로는 공인인증서 등에도 적용하여 고객의 생명과 재산을 더욱더 안전하게 지킬 수 있는 시스템으로의 확장과 이에 따른 범죄예방시스템과의 연계 가능성에 대한 연구가 필요하다고 본다.

참고문헌

- [1] 전돈수. "상황적 범죄예방이론을 응용한 은행 강도 예방대책". 한국경찰연구학회. 한국경찰연구회지, Vol.2005, No.1. pp.53~73. 2005.03.
- [2] 박희환. "새로운 Internet-Banking 인증 방안 연구". 숭실대학교 정보과학대학원 정보보안학과 석사학위논문. 2008.12.
- [3] 서병삼, 한계섭. "인터넷뱅킹 확산에 따른 금융전산망 보안방안 연구". 한국경영정보학회. 한국경영정보학회지, pp.433~441. 1998.11.