




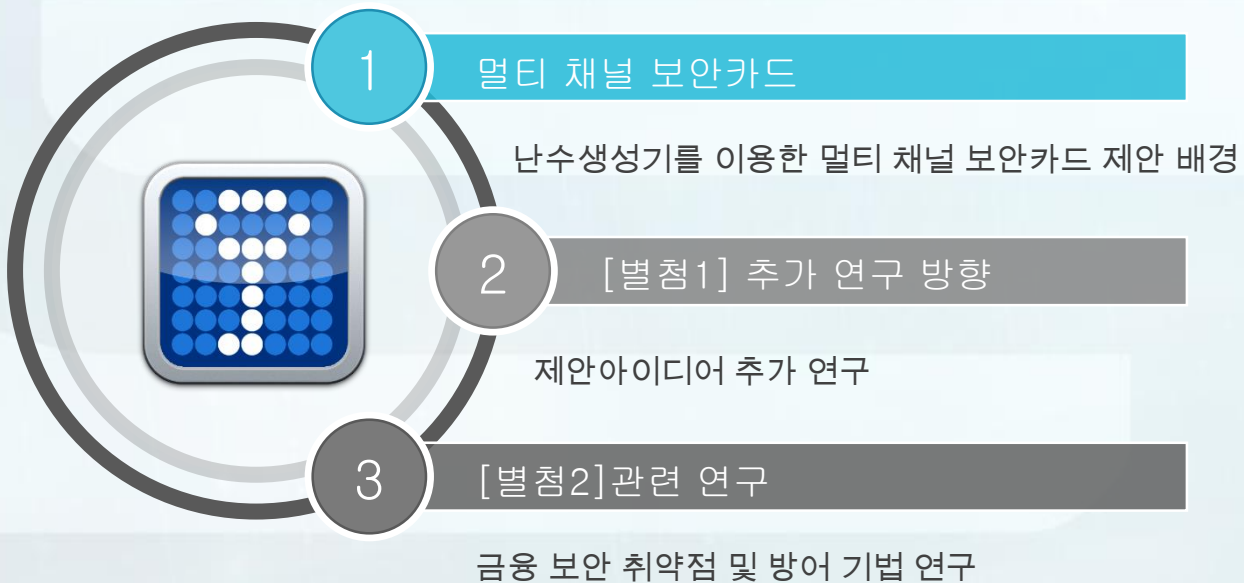
2014 국가암호기술 공모전[1-B 분야]

난수 생성기를 이용한 멀티 채널 보안카드의 설계





발표내용



개요



멀티채널 보안카드

- 보안카드의 **비밀정보**를 **두 개의 채널**로 나눠서 보관



Channel 1. 물리적 비밀번호 카드

기존의 보안카드에 비밀번호를 절반만 표시



Channel 2. 동적 비밀번호 생성 앱



보안카드 사용 시점에 나머지 비밀번호를 생성



보안카드 비밀번호

멀티채널 보안카드

2		9		16		23		30	
3		10		17		24		31	
4		11		18		25		32	
5		12		19		26		33	
6		13		20		27		34	
7		14		21		28		35	



멀티 채널 보안카드



제안하는 보안카드 형태

보안카드 번호 인덱스

보안카드 번호

No.									
1	7073	2	7021	3	7191	4	2951	5	9766
6	4775	7	4831	8	1533	9	1875	10	3165
11	5453	12	9997	13	8498	14	9576	15	9094
16	9270	17	2001	18	9572	19	1748	20	4087
21	0869	22	6152	23	4255	24	1228	25	2868
26	6989	27	8131	28	6774	29	1557	30	6890
31	2693	32	4953	33	4631	34	5987	35	8533

무작위로 공백 생성

No.									
3	7	2	7	1	7	2	9	2	9
6	4				8	3	1	8	1
1	5	4			9	8		9	
26		2	7		0	8	9	1	4
1		8	9	2	6	5	4	1	2
16	6		8	9	2	8	1	2	6
0		6			4	5		3	8

- 보안성 향상을 위해 보안카드 번호와 인덱스 위치를 무작위로 배치
- 물리적 보안카드에서 번호와 인덱스를 일부만 표시하고 나머지는 구멍이 뚫린 형태로 배포하여 보안카드 분실 시에도 전체 보안카드 번호의 유출방지

멀티 채널 보안카드

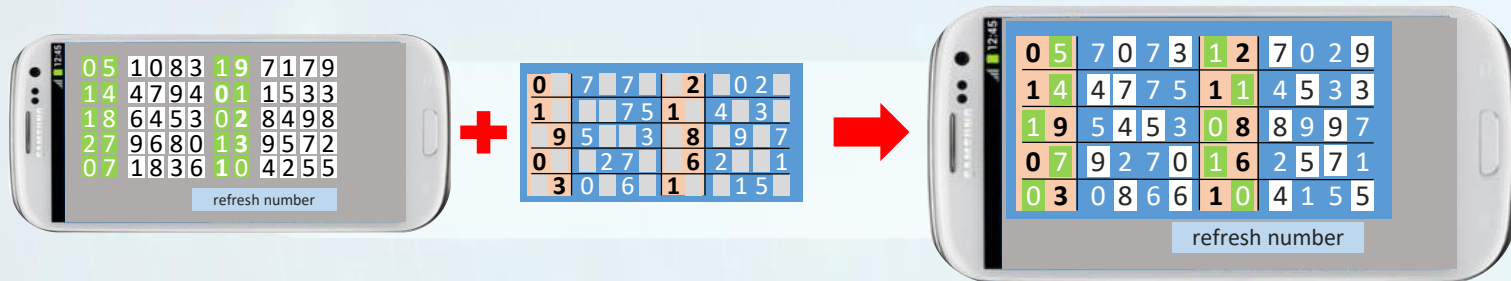


동적 보안카드 비밀번호 생성 어플리케이션



- 멀티채널 보안카드와 동일한 화면 크기를 가지는 동적 보안카드 번호 생성 어플리케이션
- 어플리케이션 화면 위에 멀티채널 보안카드를 올려 놓게 되면 공백 부분에 보안카드의 나머지 비밀번호가 표기되도록 설계
- 어플리케이션을 통해 생성되는 보안카드 비밀번호는 앱 구동 시 또는 재생성 버튼(Refresh Numbers) 클릭 시 난수생성기로부터 새로운 값 생성

동작방식



Step1. 보안카드 번호 생성 앱을 통해
보안카드 비밀번호 생성

Step3. 동적으로 생성된 비밀번호 확인

Step2. 보안카드를 화면에 올리기

※ 휴대폰을 통해 생성되는 보안카드 정보는 **온라인** **뱅킹 서버와 휴대폰**이 초기에 **상호간에 분배한 seed값을 통해 난수값을 생성**하는 기법을 사용

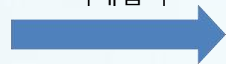
※ seed값은 타임스탬프, 카운터 혹은 사전 정의된 비밀키 값을 이용 가능

사용시나리오

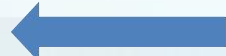


멀티채널 보안카드의 온라인뱅킹 사용방법

1. 금융서비스 접근,
거래입력

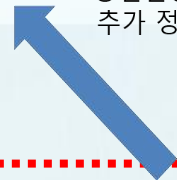


2. 보안카드 정보
입력 요청



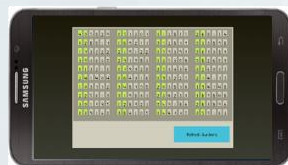
온라인 뱅킹 페이지

5. 확인한 난수 입력 및
공인인증서 비밀번호 입력 등
추가 정보 입력 후 거래 완료



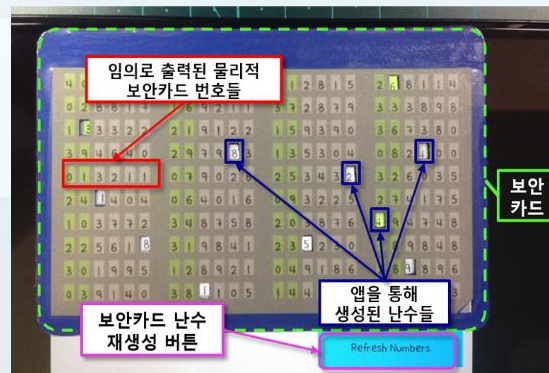
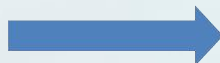
멀티채널 보안카드 인증 과정

3. 난수 생성 앱
실행



난수 생성 앱 구동 스마트폰

4. 보안카드로
입력 번호 확인



스마트폰 화면에 카드를 갖다 대어
입력할 난수 확인

데모 구현



타킷장비

[성능 비교]

특성	갤럭시 S1	갤럭시 S2	갤럭시 S3	갤럭시 S4	갤럭시 S5	IRON
해상도	480X800	480X800	720X1280	1920X1080	1920X1080	1920X1080
디스플레이	4인치 슈퍼 AMOLED	4.3인치 슈퍼 AMOLED Plus	4.8인치 HD 슈퍼 AMOLED	5인치 풀HD 슈퍼 AMOLED	5.1인치 FHD 슈퍼 AMOLED	5.0인치 HD
CPU	1GHz 싱글	1.2GHz 듀얼	1.4GHz 쿼드	1.6GHz 옥타	2.5GHz 쿼드	1.7GHz 쿼드

[실물 크기비교]





보안성

- 물리적 보안카드에 집중되어 있던 보안카드 **비밀정보**를 **두 개의 서로 다른 채널** (물리적 보안카드, 스마트 폰)에 **할당**
⇒ **비밀 정보를 분산하여 보안카드 유출로 인한 문제를 최소화**
- 보안카드 **비밀정보**의 값이 **사용 시점마다 변경**
⇒ **휴대폰의 가상 보안카드가 노출되어도 해당 정보는 단 한 번만 사용이 가능하고 그 다음 세션에서는 사용이 불가능**



신속성


- 기존의 온라인뱅킹 방식에서 추가적인 채널에서의 결합된 **비밀정보 확인을 위한 작업** 부하가 발생
⇒ **약 5~10초 정도 부하로 사용자의 불편함 최소화**



Q & A



감사합니다



발표내용

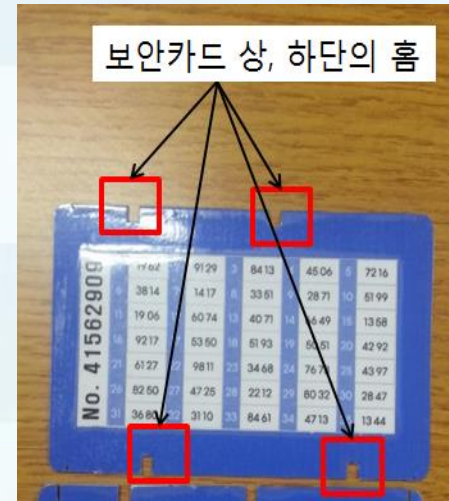


추가 연구 방향



보안카드 기능 추가

- 피싱/파밍공격 방지를 위한 온라인 뱅킹 사이트 인증기능이 추가된 보안카드
- 보안카드의 상,하단 여백 부분의 디자인을 변경
- 사용자가 간단한 테스트를 통해 접속한 사이트의 진위여부를 판별

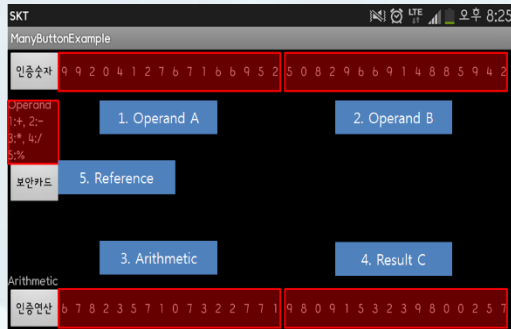


[가정 1] 보안카드 각각 다른 디자인의 보안카드 발급

[가정 2] 인터넷뱅킹 서버는 사용자의 보안카드 디자인 정보와 초기 Seed 값을 공유

향후 연구 방향

[방법 1] 간단한 연산을 통한 인증



[인증방법]

보안카드를 인증화면에 올린 후,
상단 두 개의 홈의 operand,
하단 좌측 홈의 연산자를 통해 연산 후
하단 우측 홈에 표시되는 연산결과 확인

[결과확인]

연산결과가 화면에 표시되는
연산결과와 일치하면 인증 성공

[방법 2] 출력되는 색상정보를 통한 인증




[인증방법]

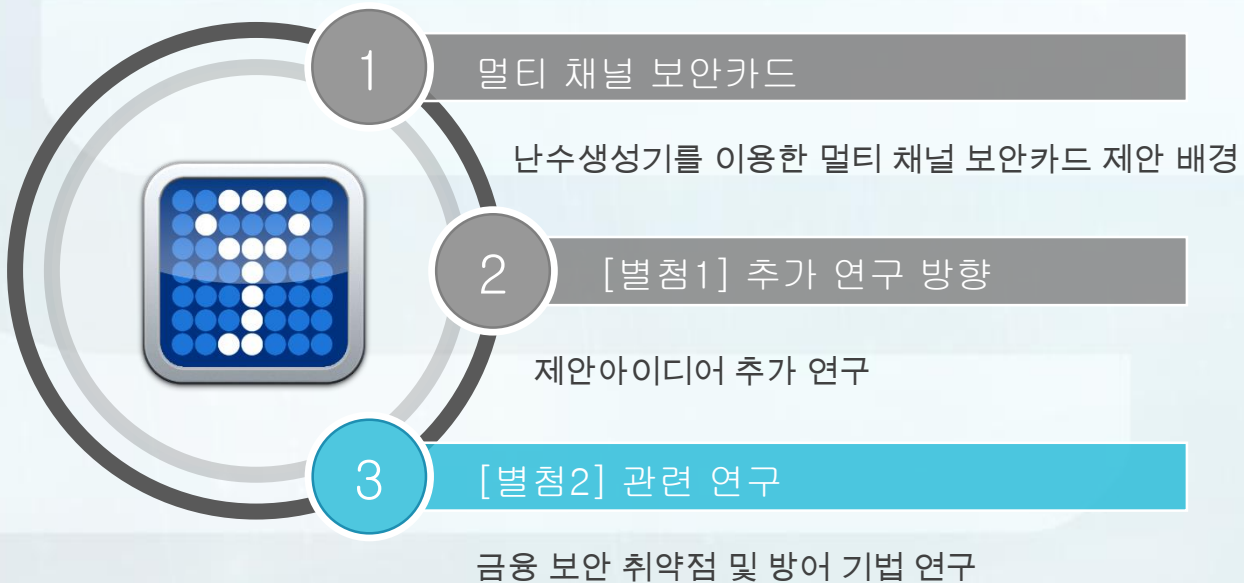
보안카드를 인증화면에 올린 후,
상단 2개, 하단 2개의 홈에 표시되는
색상을 확인

[결과확인]

모든 색상이 **동일**하면 인증 성공



발표내용



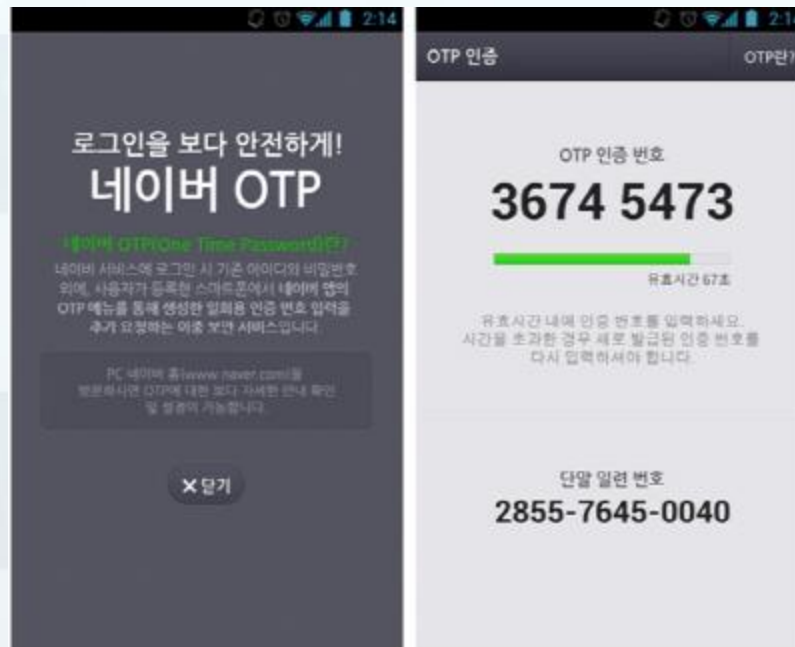
최신 금융보안 기술

- PIN(Personal Identification Number)
 - 사용자와 시스템 사이에 사용하는 비밀번호
 - 시스템에 사용자가 접근 시 신분 인증을 위해 사용
 - PIN은 카드에 수동으로 카드 보유자에 의해 시스템에 입력
 - 온라인 이체등과 같은 금융 거래 시 사용자 인증을 위해 사용
 - 온라인 뱅킹 시스템은 카드 발급사와 은행, 업체들간의 상호 운용성을 기반으로 설계됨



최신 금융보안 기술

- OTP(One-Time Password)
 - 로그인이나 금융거래와 같이 비밀번호가 필요한 경우 한번의 이벤트에 대한 검증용으로 사용되는 비밀번호
 - 기존의 비밀번호 체계와 달리 replay attack에 대한 방어가 가능



최신 금융보안 기술

- OTP 공유정보 생성방식
 - 시도 응답(Challenge-response)방식: 서버로부터 제시되는 시도 값을 얻은 후 그 값을 특정한 알고리즘에 넣어 수행한 뒤 나오게 되는 값을 응답으로 서버에 입력하여 정당한 사용자인지 확인
 - 시간동기화(Time-Synchronous)방식: 서버와 OTP단말기의 시간을 동기화하여 특정한 시간 간격에 따라 다른 OTP를 생성해 내는 방식
 - 이벤트 동기화(Event-Synchronous)방식: 서버와 OTP단말기 간에 공유된 카운터를 유지하며 해당 값에 따라 OTP값을 생성



최신 금융보안 기술

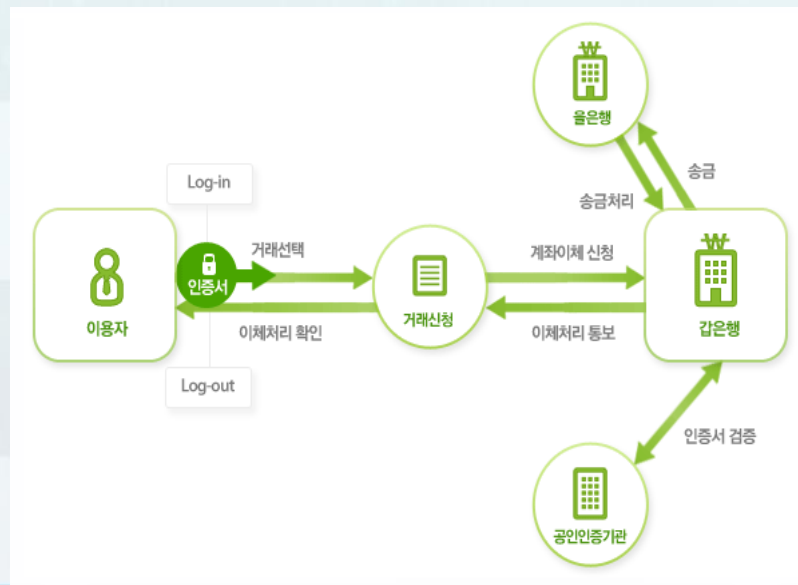
• 공인인증서

- 전자 서명의 검증에 필요한 공개키에 소유자 정보를 추가하여 만든 전자 신분증으로써 개인키와 한 쌍으로 존재
- 공인인증서는 전자 거래 시 신원확인, 문서의 위/변조, 거래사실 증명 등을 위해 사용하므로 일련번호, 발행기관 식별명칭, 유효기간과 같은 정보를 포함하게 됨

주요 구성요소	설명
일련번호	공인인증서 일련번호
발행기관 식별명칭	공인인증기관 식별명칭
유효기간	공인인증서 유효기간 시작일과 만료일을 명시
소유자 식별명칭	공인인증서 소유자의 실명을 포함한 식별명칭
공개키	공인인증서 소유자의 공개키
공개키 사용목적	공개키의 사용목적을 명시(전자서명, 암호화 등)
인증서 정책	공인인증서 발행기관이 인증서를 발행하는데 적용한 인증서 정책과 인증업무 준칙을 명시
발행기관의 서명값	위의 내용이 진실임을 증명할 공인인증기관의 전자서명 값

최신 금융보안 기술

- 공인인증서를 통한 금융거래 방법
 - 공인인증서와 비밀번호를 통해 사이트에 로그인
 - 계좌와 금융서비스 정보를 입력하고 거래를 요청하면 금융기관에서는 사용자 인증을 위해 보안카드 정보를 요구
 - 전자서명을 위해 공인인증서와 공인인증서 비밀번호를 다시 한 번 요청
 - 금융기관은 입력 받은 인증서를 공인인증기관으로부터 검증을 하고 검증 결과에 따라 금융거래를 진행



최신 금융보안 기술

- 보안카드를 통한 금융 보안
 - 보안카드에는 다수의 난수와 일련번호가 적혀있는 난수표로서 사용자에게 1매씩 발급하며 은행에서는 사용자가 입력한 번호의 정당성을 평가
 - 공격자의 악의적 금융서비스 이용을 방지

일련번호: 04952174

1	4597	8	1212	15	0102	22	4888	29	2845
2	1346	9	1313	16	1269	23	4882	30	3244
3	5326	10	4466	17	9546	24	1344	31	2288
4	1975	11	12	24	11	25	5511	32	7547
5	4555	12	24	11	26	1999	33	5144	
6	2311	13	2928	20	2113	28	74	68	
7	6249	14	3444	21	1111				

은행코드: 경남 039 경남은행

보안카드 [12]번 비밀번호 네자리 중 앞 두자리

24

**

보안카드 [28]번 비밀번호 네자리 중 뒤 두자리

**

68

신종 금융사기

• 피싱

- 개인정보와 낚는다의 합성어로 전화, 문자, 메신저, 가짜사이트 등의 수단을 통해 금융거래 정보를 요구하거나 피해자의 금전을 이체하도록 함
- 공격방법은 악의적 공격자가 사용자에게 문자나 이메일을 통해 피싱사이트 주소를 전송하고 사용자는 피싱사이트에서 자신의 비밀번호를 입력하게 됨으로써 공격자는 사용자의 비밀정보를 확인할 수 있음



신종 금융사기

• 파밍

- 피싱과 조작의 합성어로 악성프로그램에 감염된 PC를 조작하여 피해자가 정상 사이트로 접속하더라도 가짜 은행사이트로 접속을 유도하여 금융 거래정보를 빼낸 후 금전적인 피해를 입히는 수법
- 공격자는 악성코드를 사용자에게 전송하게 되고 사용자는 이를 자신의 컴퓨터에 깔게 됨
해당 악성코드는 적합한 사이트의 주소를 변경하여 악의적 사이트로 유도하여 접속한 사용자가 의심없이 자신의 정보를 입력하게 함

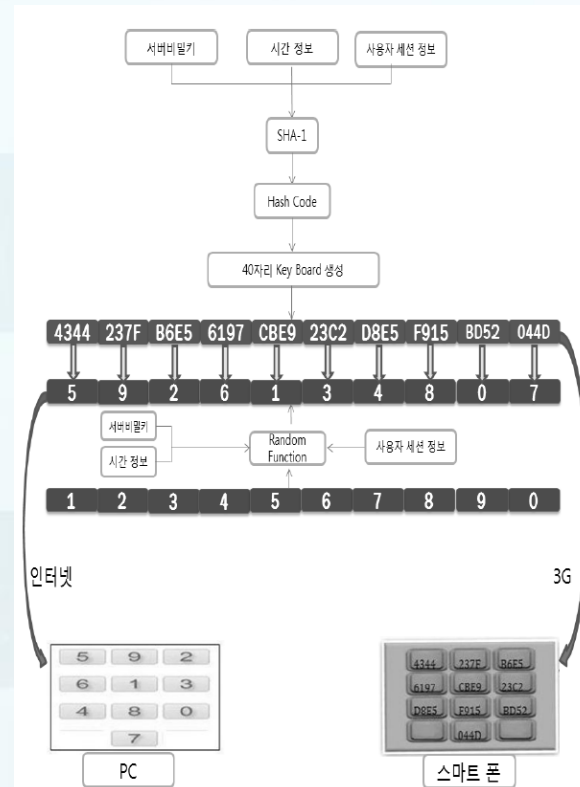


신종 금융사기

- 사례1 상품 구매 후 피해자의 계좌를 이용해 상품 결제
 - 피싱 사기범들은 가짜은행사이트를 만든 후 인터넷 बैं킹 정보를 빼돌리고 이를 이용하여 현금화가 쉬운 귀금속이나 상품권을 구매함. 구매한 상품에 대한 대금은 직접 판매업체에게 송금하도록 함
- 사례2 채팅, 발신번호 변작을 통한 추가인증 정보 탈취
 - 은행 또는 은행직원으로 속여 피싱사이트 내 실시간 채팅창을 통해 전자금융사고 예방을 위해 ARS 인증이 필요하다고 하여 인증번호를 가로채 피해자의 예금을 무단 이체하는 수법을 사용
- 피싱/파밍 사기 수법에 대한 강력한 예방책이 부재하며 주기적인 비밀번호 변경, URL 확인, 카드정보/인증정보 누설 금지 등 일반 사용자들의 주의가 당부됨

신종 금융사기 방어 기법

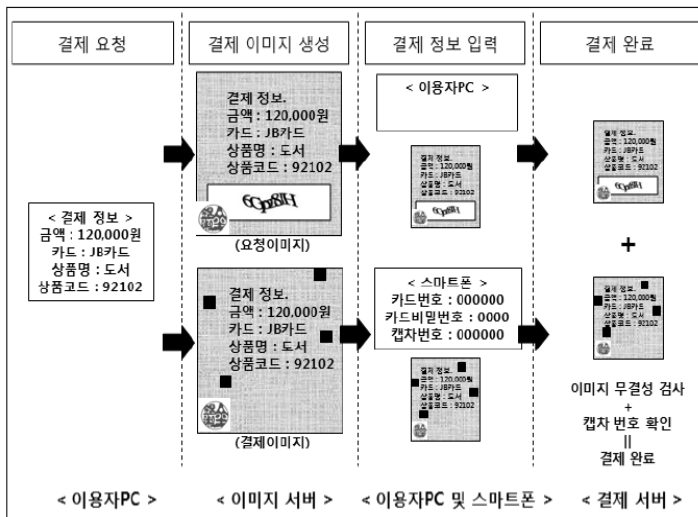
- 다중채널 기반의 안전한 금융거래 입력방식
 - PC 혹은 스마트폰만을 이용한 거래는 공격자에게 단말기가 해킹당한 경우 정보가 유출될 수 있는 문제점을 가짐
 - 정보유출을 방지하기 위하여 다중 채널을 이용한 입력과 출력을 분리하는 새로운 접근 방법을 통해 입력방식의 안전성을 높이는 효율적인 방안이 제시됨
 - 하지만 난수 값이 전송되더라도 특정 난수가 2번 이상 반복되는 경우 비밀번호의 패턴이 공격자에게 노출될 수 있는 문제점을 가짐



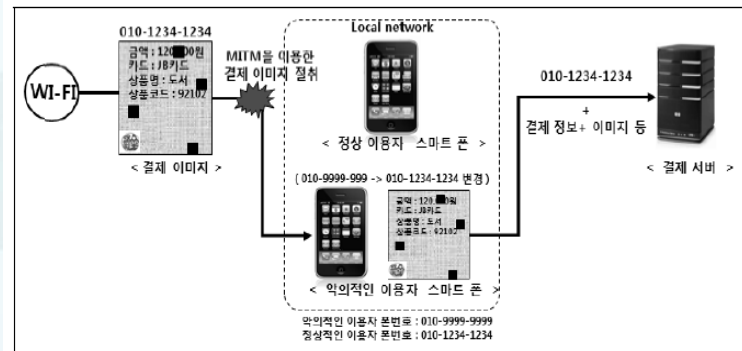
신종 금융사기 방어 기법

- 스마트폰을 활용한 안전한 온라인 승인시스템 연구
 - 현재 보안 솔루션은 다양한 환경 상에서의 호환성을 제공하는 것이 어려움
 - 서버에서 생성된 이미지 정보를 이용하여 결제를 수행
 - 하지만 보안이 취약한 와이파이를 통한 이미지 전송은 중간자에 의해 이미지가 조작될 수 있는 문제점을 가짐

시스템 설계



취약점



신종 금융사기 방어 기법

- 전자금융거래 환경에서 보안카드 실수입력방지기법 적용을 통한 피싱/파밍 사고 방지 방안
 - 사용자의 보안카드의 디자인과 입력 인덱스값을 수정하여 사용자가 사이트의 진의여부를 판단하도록 제안됨
 - 실수입력방지 보안카드는 보안 카드 번호에 마스킹을 적용하여 사용자마다 상이한 형식으로 발급

기존 보안카드

신한보안카드 NO.12345678
이 카드는 타인에게 노출되지 않도록 주의하시기 바랍니다.

1	33 01	7	07 76	13	46 76	19	40 78	25	52 93
2	34 76	8	63 66	14	24 91	20	71 72	26	54 30
3	77 75	9	14 54	15	28 52	21	67 83	27	02 74
4	15 27	10	51 31	16	83 87	22	06 69	28	81 97
5	47 12	11	52 12	17	57 78	23	86 94	29	14 89
6	03 16	12	71 03	18	03 51	24	82 00	30	48 16

실수입력방지 보안카드

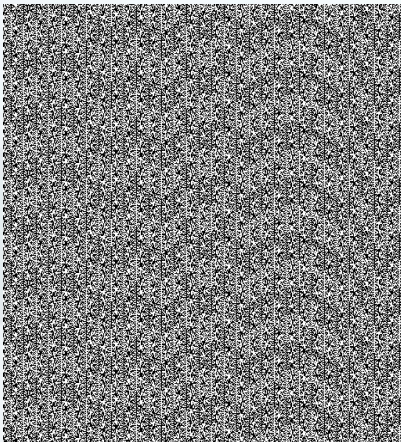
신한보안카드 NO.12345678
이 카드는 타인에게 노출되지 않도록 주의하시기 바랍니다.

1	33 01	4	34 76	7	77 75	10	15 27	13	47 12	16	03 16	19	46 76	22	24 91	25	28 52	28	83 87
2	07 76	5	63 66	8	14 54	11	51 31	14	52 12	17	71 03	20	40 78	23	71 72	26	6/ 83	29	06 69
3	07 76	6	63 66	9	14 54	12	51 31	15	52 12	18	71 03	21	40 78	24	71 72	27	6/ 83	30	06 69

난수 생성기

- 암호화에 사용되는 비밀 키 값은 공격자가 예상할 수 없는 임의의 값이 선택 및 사용되어야 함
 - PRNG는 seed라 불리는 초기값과 알고리즘의 상태를 이용하여 난수를 생성
 - TRNG는 예측할 수 없는 실물을 기반으로 하는 난수생성기
 - 암호화 요건을 만족시키는 PRNG를 CSPRNG로 명시함

PRNG



TRNG

