PHI ATTACK

REWRITING THE JAVA CARD CLASS HIERARCHY

Jean DUBREUIL
j.dubreuil@serma.com

Guillaume Bouffard
guillaume.bouffard@ssi.gouv.fr

SERMA
SAFETY & SECURITY

AGENDA

Java Card Platform

- Java Card Security Model
- Loading process description

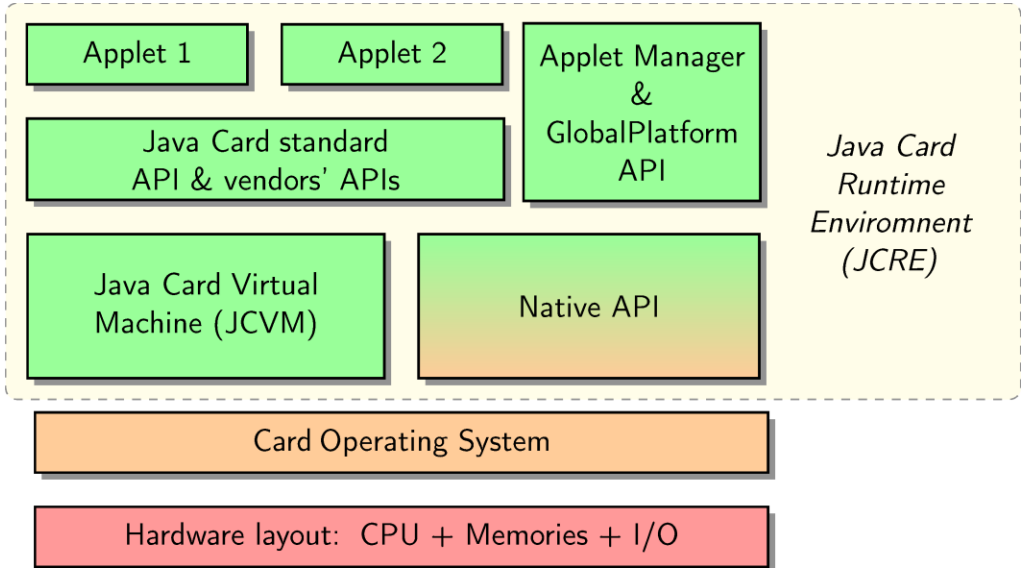
PhiAttack

- Fooling the loading mecanism
- Exploitation
- How to prevent from such an attack ?

JAVA CARD SMART CARD

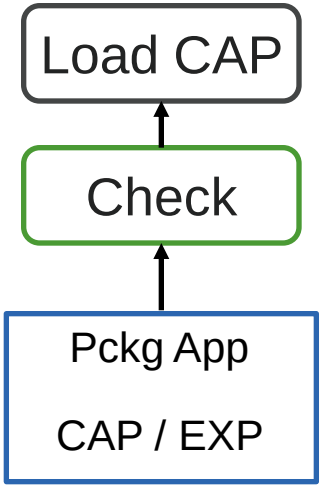
Java VM embedded on secure component (constrained device)

- Specified by Oracle
- Applications segregated by firewall
- **Latest products embedd version 3.0.5**
- Loading specified by GlobalPlatform



APPLET LOADING

- Issuer (ISD / Authorized Management) -> Trusted
- Verification Authority (VASD / Mandated DAP) -> Trusted
  - Verification performed based on product security guidance (BCV, etc.)
- Application developer
  - When trusted -> everything is fine
  - When not trusted -> only VA prevents malicious code loading



PHI ATTACK – BIBLIOGRAPHY (1/2)

Malicious Code on Java Card Smartcards – Mostowski and Poll – 2008

- Abuse Shareable interface using modified EXP file
  - server.cap, server.exp
  - client.cap -> compiled with modified_server.exp
  - Allows type confusions
- Verification Authority keeps all exp files corresponding to loaded cap
  - Verification detects that client.cap is not consistent with server.exp

PHI ATTACK – BIBLIOGRAPHY (2/2)

Accessing Secure Information using Export file Fraudulence – Bouffard, Khefif and Lanet – 2013

- Man in the middle
  - Malicious app developer: provides a fake API
  - Victim app developer: app.cap -> compiled with fake API export files
  - Allows interception of any call to API methods
- Verification Authority has legitimate API export files
- Difficult to send fake export files to the victim developer

PHI ATTACK

Attack model

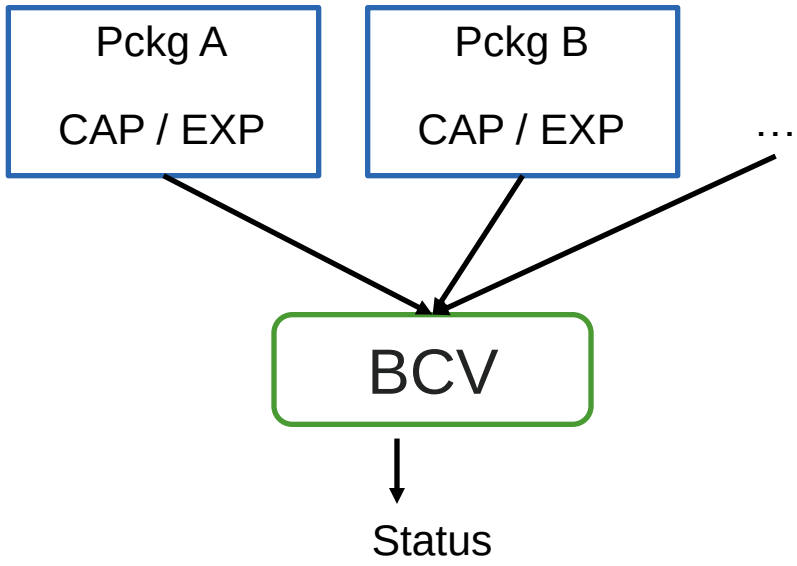
- CAP and EXP files come all from malicious App developer
- No file modification: they are consistent

- Verification Authority cannot detect malicious code
  - If only BCV is used
  - AND if exp files provided are in version 2.2 (specified in Java Card 3.0.5)

JAVA CARD IMPORT MECHANISM

Asymmetry in import mechanism

- CAP file
  - Imported packages are listed in Import component
  - Referenced by AID value
  - For instance “A0 00 00 00 62 00 01”
- Export file
  - Referenced by the fully qualified name
  - For instance “java/lang”



ATTACK SET-UP (1/3)

Pckg: library / AID: DEADBEEF**01**

```
class Phi {
  Object confusion(Object obj){
    return obj;
}}
```

Pckg: library / AID: DEADBEEF**02**

```
class Phi {
  Object confusion(short s){
    return null;
}}
```

ATTACK SET-UP (2/3)

Pckg: library / AID: DEADBEEF**01**

```
class Phi {
  Object confusion(Object obj){
    return obj;
}}
```

Pckg: library / AID: DEADBEEF**02**

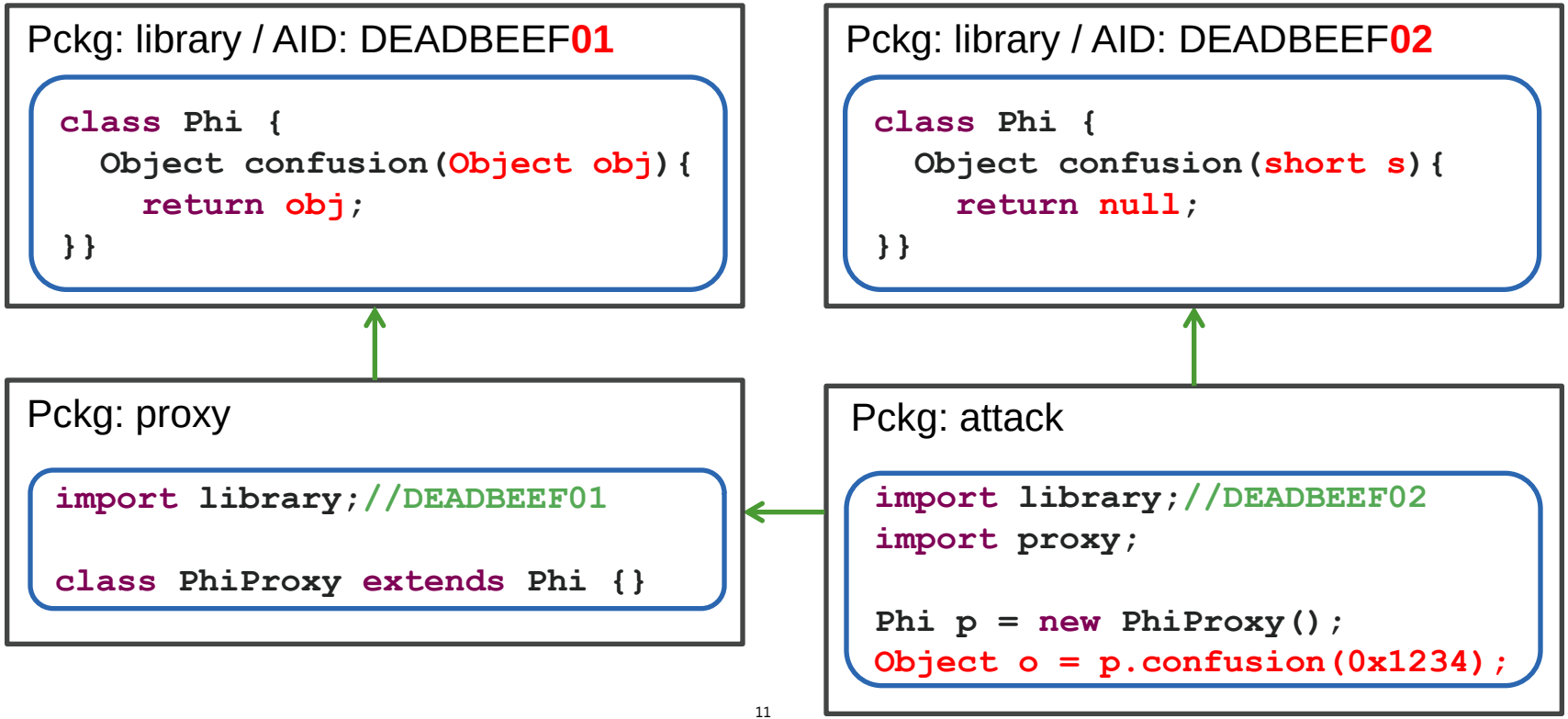
```
class Phi {
  Object confusion(short s){
    return null;
}}
```

Pckg: proxy

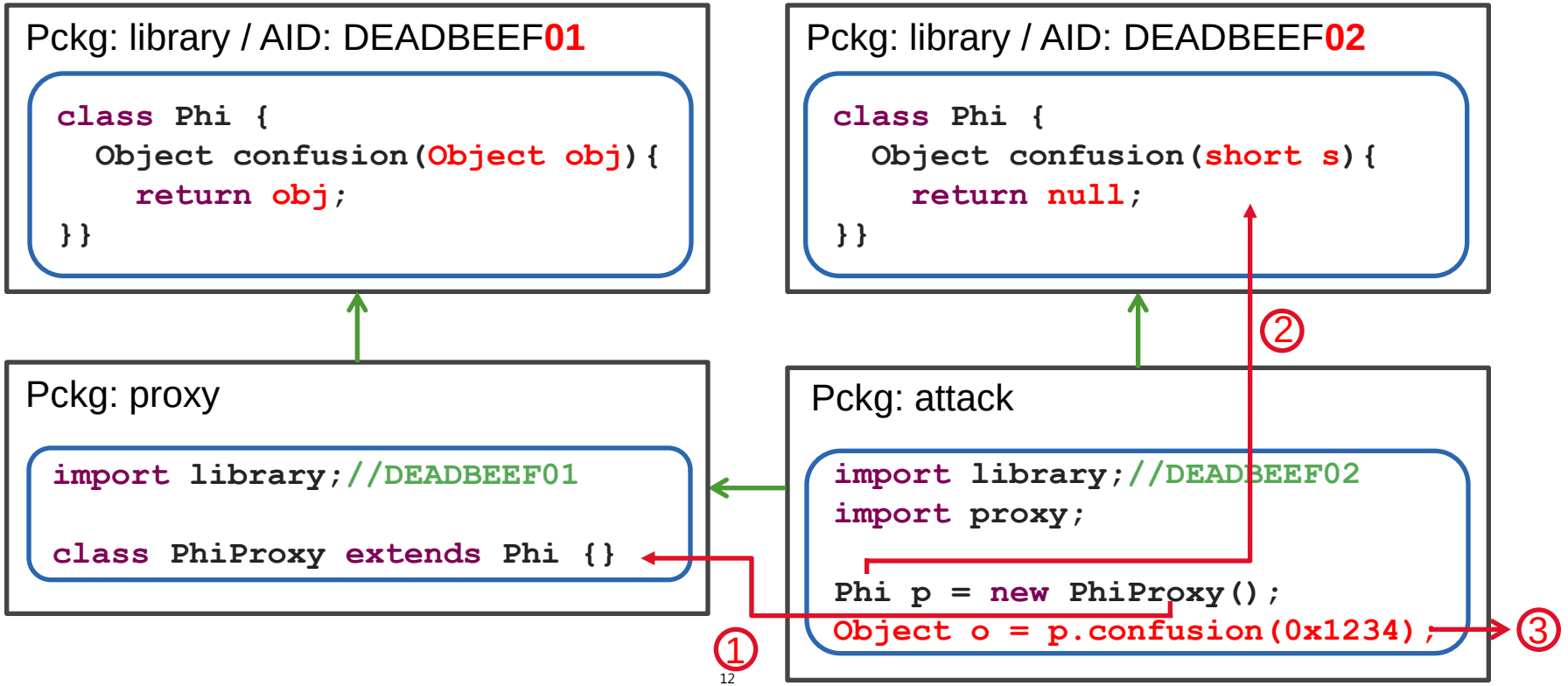
```
import library;//DEADBEEF01

class PhiProxy extends Phi {}
```

CAP file references DEADBEEF01
EXP file references library

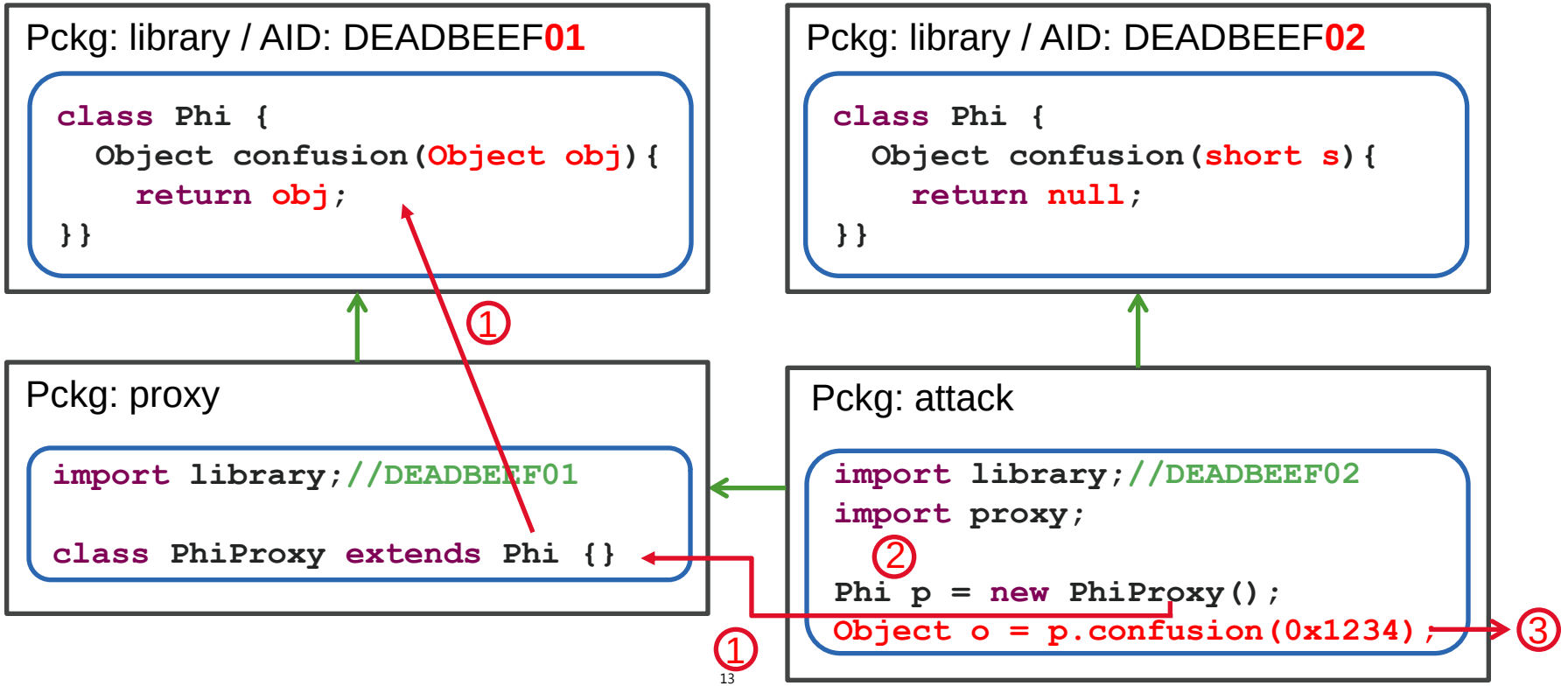
ATTACK SET-UP (3/3)



BCV VIEW



AT RUNTIME



PHI – VARIATIONS

- Principle can be applied everywhere
  - On Java Card standard API
  - Even on java.lang, with Object (but often forbidden)
- Going deeper
  - Different number of methods
  - Overflow in CAP structures, may be powerful
  - But more implementation dependent

PHI – SUMMARY

- Not detected by BCV
- Due to the lack of information in exp file in version 2.2
- Not full attack, only a potential weakness
  - No assets disclosure,
  - But a first step for further investigations:
    - Stack overflow/undeflow
    - Type confusion
    - Overflow in CAP structures
    - Etc.

PHI – COUNTERMEASURES

- Check the AID consistency

- How ?
  - Manually or with a dedicated tool
    OR
  - Force usage of EXPort file version 2.3
    - Defined in Java Card 3.1
    - Each imported package is referenced by its name **AND** its AID
    - But not always available (for instance GlobalPlatform)

THANK YOU FOR YOUR ATTENTION

Jean DUBREUIL
j.dubreuil@serma.com

Guillaume Bouffard
guillaume.bouffard@ssi.gouv.fr

SERMA
SAFETY & SECURITY

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI