

PV204 Phase 3 slides

The review

manual code
inspection

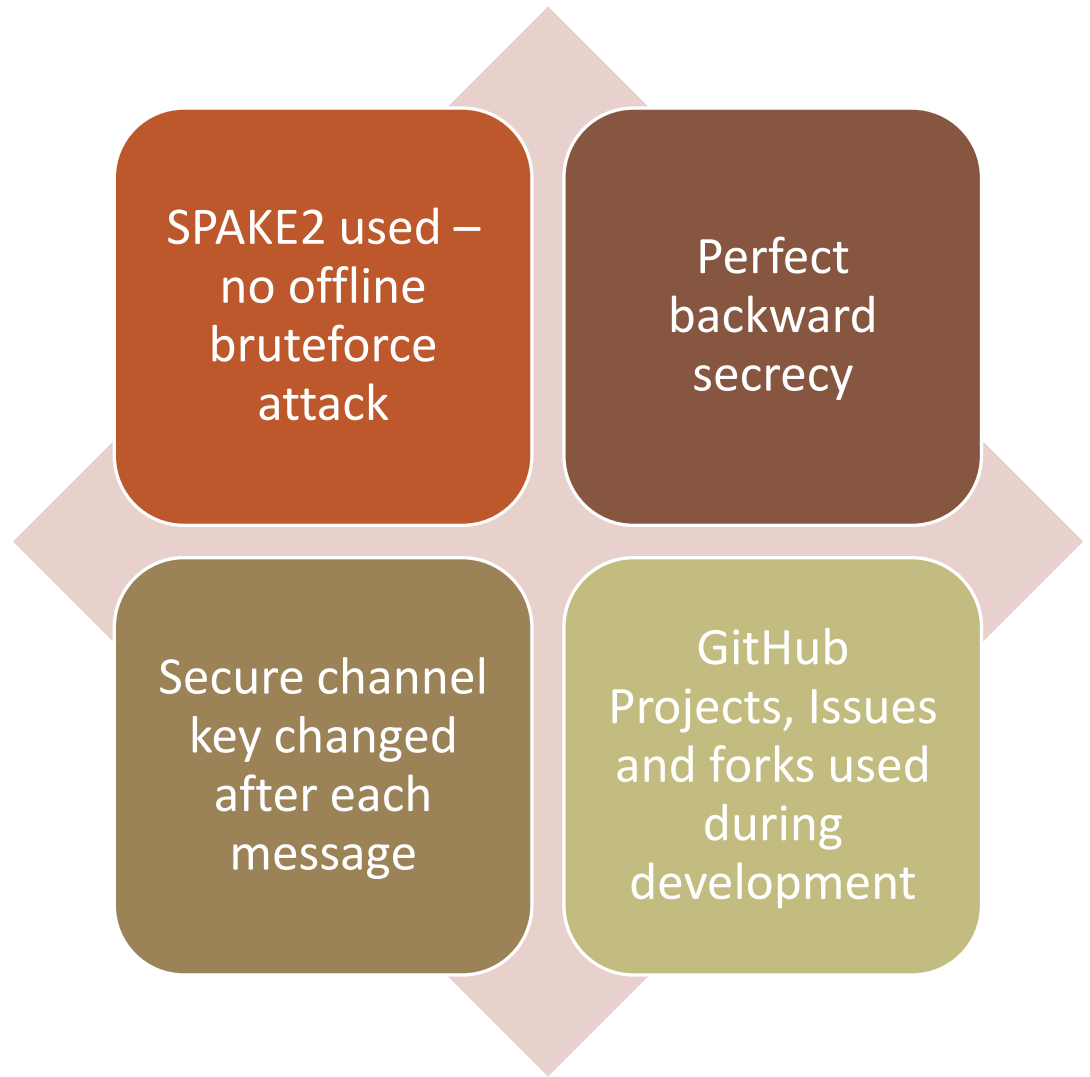
13 GitHub Issues
opened

Description +
remediation
provided

Both protocol and
applet logic
implementation
attacked

(Java Card) Code
quality discussed

The good



Implementation issues

Full-blown Java libraries in applet

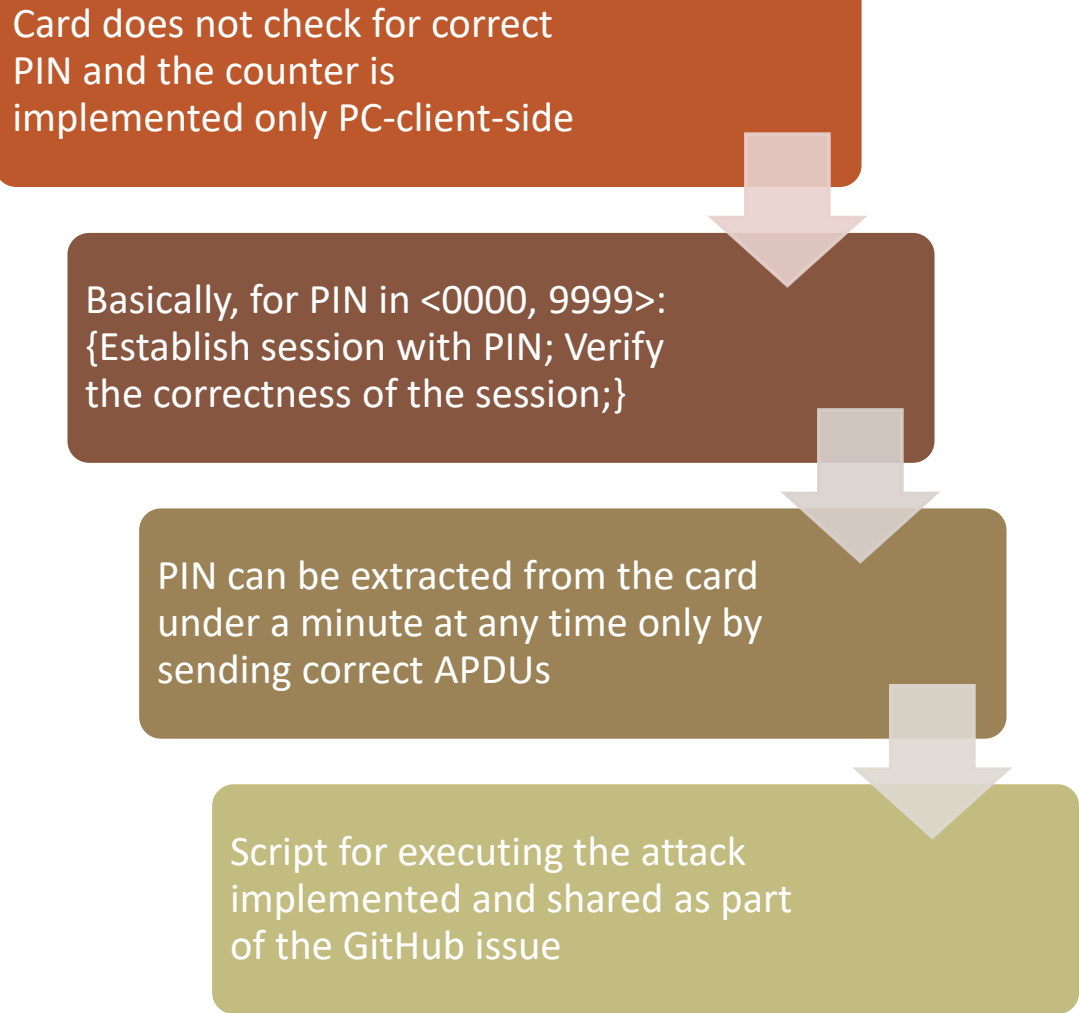
Java Card libraries in PC client

Some arrays in ROM

Allocation outside constructor

Not reusing objects

Card does not check for correct PIN and the counter is implemented only PC-client-side



```
graph TD; A[Card does not check for correct PIN and the counter is implemented only PC-client-side] --> B[Basically, for PIN in <0000, 9999>: {Establish session with PIN; Verify the correctness of the session;}]; B --> C[PIN can be extracted from the card under a minute at any time only by sending correct APDUs]; C --> D[Script for executing the attack implemented and shared as part of the GitHub issue];
```

Basically, for PIN in <0000, 9999>:
{Establish session with PIN; Verify the correctness of the session;}

PIN can be extracted from the card under a minute at any time only by sending correct APDUs

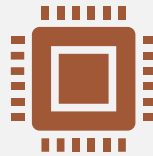
Script for executing the attack implemented and shared as part of the GitHub issue

PIN extraction

PIN hash extraction from memory



Stored unencrypted
on the card



Stored unencrypted
and redundantly on
the PC



Protected only by
simple SHA hash

Unlimited
session
length +
secret
extraction
from RAM



The session cannot be explicitly terminated



The session never ends on the card



The secret changes, but predictably



If the secret for encryption is leaked once,
the attacker can eavesdrop and decrypt all
the communication



Could be used to operate the card and leak
data from it indefinitely

Thank you and
passing the word
to Daniel

