PIV Card Enhancements

Approaches for minimizing the computational costs of FIPS 140-2 POST

Apostol Vassilev,
Security Testing Research Team Lead
Acting CMVP Manager
March 3, 2015

Background – GSA experimental results and recommendations

- **GSA PACS Analysis and Recommendations reported in October 2014:**
  - *The wall clock time for PACS with smart cards is unacceptably long:*
    - **4.0 to 4.8 seconds** for a card that it has not recently seen;
    - **3.5 to 4.4 seconds** for a card it has recently seen and has cached the Card Auth Cert.
  - *A typical breakdown of the total time looks like this:*
    - Performing the challenge/response (~1.2 sec)
    - Reading the Card Auth Cert (~0.6 sec)
    - FIPS 140-2 POST (~0.6 to 1.0 sec)
    - PACS access decision (~0.9 sec)
  - *Suggested directions for improvement*
    - **Short term:** eliminate wasted steps, optimize necessary steps
    - **Medium term:** move to faster crypto (ECC) and optimize POST

CMVP work with the smart card industry on POST optimization

- **The CMVP engaged with the industry to analyze the problem and propose ways for improvements**

  - ***Analysis***
    - The typical current POST implementation on smart cards is in the *platform*
      - Implemented once for all applets, independent of use-case.
    - This architecture is quite computationally sensitive and costly when used with un-optimized readers – recall GSA analysis
      - POST is particularly costly for use-cases based on *few* crypto algorithms
    - ***IG 1.7 : Multiple Approved Modes of Operation*** is unknown and not used

Preliminary Results and Next Steps

- ***Candidate architectures produced by several companies***
  - Promisingly compliant but final determination still pending, waiting on formal submission
  - Hold potential for *significant* performance improvement of POST for *specific* use-cases
    - Especially for ECC-based use-cases
  - Hold potential for performance improvements even when used with non-optimal readers
    - POST is invoked much later in the power-on cycle so bad reader commands do not incur the overhead of POST
    - POST performance is stable and largely independent of the rest of the PACS infrastructure

Preliminary Results and Next Steps

- ***NIST will <u>not</u> publish reference architectures***
  - We believe this task is better left to the industry: individual companies, Global Platform, Smart Card Alliance, etc.
  - CMVP-NIST is open to working with the industry on vetting reference architectures for compliance.
- ***Looking ahead to potential new standards***
  - The smart card industry may benefit from lobbying ISO for reinstating EDC-based integrity check in ISO 19790
  - CMVP NIST is working on ways to allow more flexibility in testing the integrity of modules but work is still too preliminary to report.

Conclusions

- *It is possible to improve the performance of POST*
- *POST is only one piece of the puzzle so a full resolution of the performance problem requires improvements in the remaining PACS architecture components*
- *CMVP-NIST is open to working with the industry and the relevant USG Agencies to achieve a satisfactory user experience for PACS*

Points of Contact

NIST-CMVP

Apostol Vassilev, Team Lead, Security Testing Research,
Acting CMVP Manager, NIST
apostol.vassilev@nist.gov