A systematic approach to eliminating the vulnerabilities in smart cards evaluation

Hongsong Shi, Jinping Gao, Chongbing Zhang

hongsongshi@gmail.com

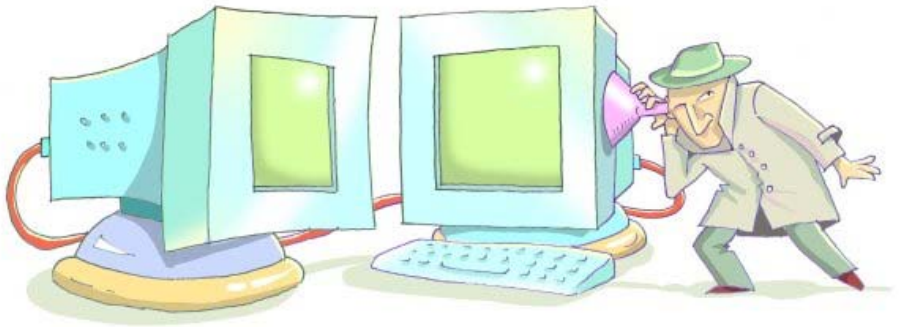
China Information Technology Security Evaluation Center

Sept., 2013

CNITSEC

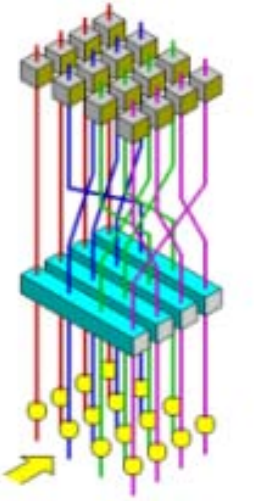
Guideline

- Motivation
- The problem-oriented analysis method
- Vulnerability analysis in the approach
- Conclusion



CNITSEC

Motivation – Security of crypto-devices



- Provable security in the *Black-box* model
  - Provable schemes in this model
    - Paillier: *IND-CPA*
    - OAEP-RSA: *IND-CCA*
    - Cramer-Shoup: *IND-CCA*
    - RSA-FDH: *UF-CMA*
    - HMAC: *UF-CMA*
    - Feige-Fiat-Shamir identification protocol: *ZK proof*
  - However, security is no guarantee *in reality*, unless the physical assumptions hold [R. Gennaro *et al*, TCC 2004]
    - read-proofness: keys, intermediates and randomness cannot be maliciously accessed
    - tamper-proofness: data and algorithm cannot be maliciously changed

CNITSEC

Motivation – Security of crypto-devices

- Provable security considering physical attacks
  - Leakage is usually a property of the crypto-devices
    - Physically observable model [S. Micali & L. Reyzin, TCC'04]
    - Memory attacks model [A. Akavia, et al.. TCC'09; M. Naor et al. Crypto'09]
    - Auxiliary input model [Y. Dodis et al.. STOC'09; TCC'10]
    - Leakage-resilient model [S. Dziembowski & K. Pietrzak. FOCS'08]
  - But implementation leakage and specificities are very difficult to capture with theoretical analysis
    - How to guarantee the leakage of the key is below the required bound of the algorithm?
    - How to guarantee the leakage function is one-way?
    - How to guarantee the unused key is not leaked?

[D. Bernstein, CHES'12]

Motivation – Assumptions

- Generic assumptions
  - Read-proof & tamper-proof
- Algorithm-specific assumptions
  - RSA
    - p, q are randomly generated primes, and |p|=|q|
    - gcd(e, \phi(pq)) = 1
  - DSA
    - (p, q, g) are randomly generated
    - Nonce is less than q and generated uniformly at random
  - Random number generator
    - Noise source is of high entropy
    - The input entropy is sufficient for randomness extraction
    - The seed is uniformly random

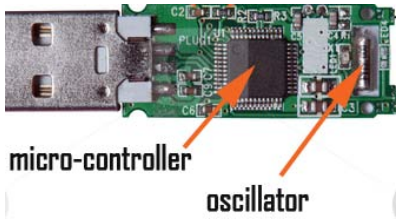
Motivation – Vulnerability analysis

- Satisfiability of algorithm-specific assumptions
  - Validate the correctness of the implementation
    - Parameter generation process
    - Algorithm implementation conformance
    - Random number generation
- Satisfiability of generic assumptions
  - Validate the correctness of the hardware & software
    - Access control on memory and functionality
    - Integrity protection of the circuit and program
    - Health checking and response mechanisms in case of faults
  - Validate the unintentional leakage
    - Characterizing the leakage of the underlying hardware
    - Countermeasures to well known physical attacks
    - Quantifying the leakage of algorithmic processing

CNITSEC

Internet banking applications of smart card

- USB & One-Time Password(OTP) token
  - Transaction signing
  - Two-factor authentication
  - Data encryption & storage
- Working paradigm
  - Inside crypto chip for
    - Data storage
    - RSA signature
    - HMAC-OTP code
    - Encryption



CNITSEC

Features of the application

- The features of the applications
  - The operating system is intertwined with the application
  - Crypto algorithms are the kernel of the application, and are implemented in both hardware and software
  - The whole product is expected to be evaluated as EAL 4+ (AVA_VAN.4) and above, while the underlying hardware may not be certified

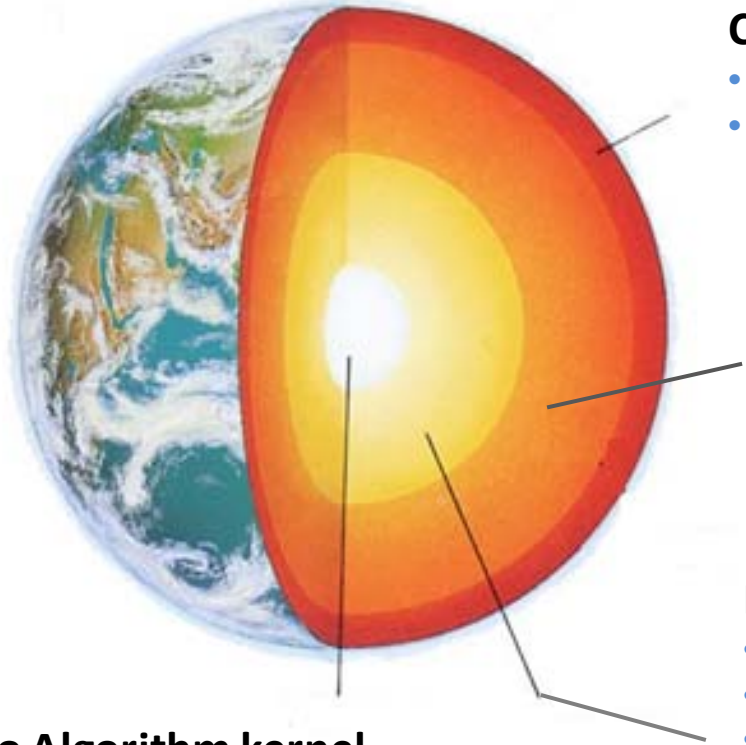
A problem-oriented approach

- Problem-oriented vulnerability analysis approach
  - It will *not* be seemed as a three-layer object as hardware, COS and application
  - The aim is to check out whether the crypto kernel is secure in reality
    - The correctness of the implementation of the algorithms
    - The effectiveness of the countermeasures
    - The effectiveness of the access control mechanism
    - The reliability of the communication
  - To reflect the above strategy, the product will be viewed as a four-layer object respectively

A methodical vulnerability analysis method!

Paradigm of the approach

TOE: smart card device



Communication interface

- Session key establishment
- Channel reliability

Data management and access control

- File management
- Authentication
- Data protection and integrity
- Power interruption handling mechanism

Physical attack countermeasures

- Memory firewall of chip hardware
- Bus scrambling and data encryption mechanism
- Intrinsic leakage characteristic
- Countermeasures to well-known physical attack
- Hardware Integrity checking mechanism
- Crypto service
- Hardware fault response mechanism
- Life-cycle transition mechanism

Crypto Algorithm kernel

- Correctness of parameter generation
- Conformance of the algorithm implementation
- Quality of the randomness

CNITSEC

Analysis- Crypto algorithm kernel

- Random number generation
  - For non-deterministic RNG, the noise source is of high entropy in theory, and the output of the RNG can pass some specific statistical tests

    [NIST SP800-22, AIS 31]
  - For deterministic RNG, the construction is provable or conforms to some specification, and the seed is securely generated and refreshed

    [NISTSP800-90, AIS 20]
- Parameters generation
  - RSA
    - Primality testing algorithm is secure in theory (i.e., the probability of the output is not prime is negligible) [J. Brandt, Asiacrypt'91]
    - p, q are generated randomly and independently each time
    - e is coprime to \phi(pq)
  - DSA
    - (p, q, g) and the nonce k are generated randomly and independently each time
    - K is less than q, and no bit is fixed for this aim [P. Nguyen et al., J. Crypt'08]

CNITSEC

Analysis- Crypto algorithm kernel

- Correctness of Algorithm implementation
  - Monte Carlo test
  - Known-Answer test

Analysis – physical attack countermeasures

- Read-proofness analysis
  - Memory firewall of the hardware
    - Memory address mapping mechanism are effective
    - Code memory and data memory are separated
    - Special functional registers are controlled
  - Bus scrambling and data encryption
    - The mechanism of bus scrambling and data encryption is effective: static, chip-specific or session-specific
    - The degree of scrambling and encryption reflects the strength in resisting the probing attacks [Y. Ishai et al. Crypto'03]

CNITSEC

Analysis – physical attack countermeasures

- Tamper-proofness analysis
  - Hardware integrity checking
    - Special functional registers integrity checking
    - Critical computational circuit integrity: modular multiplication/exponentiation, random generator, block cipher
  - Lifecycle transition control mechanism
    - Transition mechanism should guarantee irreversible property (e.g., Fuse and OTP register mechanism)
    - User mode cannot switch back to test mode and boot mode
  - Hardware fault response mechanism
    - Environment sensors: TEMP., voltage, light, frequency
    - Top mental shielding or active shielding
    - Self-destructive is necessary in the face of powerful tamper-attacks

[R. Gennaro et al.. TCC'04]

Analysis – physical attack countermeasures

- Cryptographic service
  - Parameter review and translate: RSA signing input is translated as required by the specification, e.g., PKCS #1
  - Response construction: to avoid padding oracle attacks

[R. Bardou et al.. Crypto'12, D. Bleichenbacher, Crypto'98]

- Intrinsic leakage characteristic
  - Data transition and computation leak information
  - the leakage is essentially specific to chips, thus need to characterize the leakage model of the chip
    - Signal-to-noise ratio
    - Leakage model: Hamming weight or distance, zero-value
    - Template for data transmission

Analysis – physical attack countermeasures

- Countermeasures to well-known physical attacks
  - Concrete penetration test based on well-known physical attacks

Analysis – physical attack countermeasures

- Countermeasures to well-known physical attacks
  - Evaluation of the potential leakage

Analysis – Data management and access control

- Read-proofness analysis
  - File management
    - File system: file organization, access control mechanism
    - Persistent storage management: free space allocation
  - Authentication
    - PIN verification: PIN strength control, timing analysis, administrative PIN verification
    - Counter management: power-interruption attack
    - State transition in finite state automata
  - Data protection
    - Data encryption: key encryption
    - Data destruction: key destruction

CNITSEC

Analysis – Data management and access control

- Tamper-proofness analysis
  - Data integrity
    - Code integrity: authentication code for critical code integrity
    - Key integrity: authentication code for key integrity
  - Power interruption handling
    - PIN counter refreshing
    - Key refreshing

Analysis – Communication interface

- Read-proofness analysis
  - Session key establishment
    - Two-way authentication: both of the reader and smart card authenticate each other
    - Man-In-The-Middle attack is avoided
  - Channel reliability
    - Privacy: the communication is encrypted using the session key
    - Authenticity: the communication is authenticated using the session key

Conclusion

- A methodical vulnerability analysis approach is presented
- The real security of provable algorithms can be analyzed by validating the satisfiability of the generic and algorithm-specific assumptions
  - The analysis of the algorithmic kernel is to validate the algorithm-specific assumptions
  - The analysis of the outer layers is to validate the generic assumptions of read-proof and tamper-proof


Thank you!