



*Authentication Issues:
Secure Hardware Modules,
Random Numbers, Password Expansion*

**Masaryk University in Brno
Faculty of Informatics**

Jan Krhovják

Roadmap

- Introduction
 - The importance of user authentication
 - Basic techniques of user authentication
- Hardware Security Modules
 - Architecture and the security requirements
 - Attacks on and with API
- Random and pseudorandom number generation
 - Basic principles of (T)RNG and PRNG (for ICC/SC)
 - Statistical testing of randomness
- Password-based Public Key Cryptographic Techniques
 - Draft IEEE P1363.2

Introduction

- The importance of user authentication
- Basic techniques of user authentication
 - Something you know (passwords, PINs, phrases)
 - + Easy transport, easy and fast control ...
 - Limited by human memory, can be forgotten ...
 - Something you have (key, smartcard)
 - + Hard to copy, loss easy to discover ...
 - Need of reader, user isn't recognized without object ...
 - Something you are (biometrics)
 - + Is part of a person, cannot be lost or forgotten ...
 - Accuracy, hard to measure ...
 - Combination of the above

Hardware security modules (HSM)

- Terminology – HSM, Host device, API ...
- Architecture
 - Classical von Neumann architecture
 - + Mechanisms of physical protection
 - + Generators of true random numbers
 - + Special coprocessors
 - + NVRAM
 - I/O circuits
 - Example: IBM 4758 (depicted)
- Security requirements (specified by FIPS 140-2)
 - 11 areas to testing (physical security, operating environment, key management ...)
 - Testing and independent rating it each area =>
 - 4 overall levels of security (level 4 = best security)



HSM – Attacks on and with API

- Application programming interface (API)
- Economy prevails security
 - Too many supported standards
- Three major problems of cryptographic API
 - Keys and their integrity
 - Problems with backward compatibility (DES, RC2 ...)
 - Insufficient checking of function parameters
 - Banking API and working with PINs
 - = > PIN recovery attacks
 - Insufficient enforcing of security policy
 - PKCS #11 – only set of functions

Random and pseudorandom number generation

- The need of random numbers in cryptography
 - Generating keys, random padding values ...
 - In addition to randomness => security (in the sense of unpredictability)
- Two categories of random number generators
 - (T)RNG – (True) Random Number Generators
 - Nondeterministic source of entropy
 - Output can be used directly or by PRNG as a seed
 - PRNG – Pseudo-Random Number Generators
 - Fully deterministic FSM => all randomness in seed
 - PRNG are much more faster then (T)RNG
- Statistical testing of randomness
 - Recommended by FIPS 140-2 after each restart of HSM!

(T)RNG & PRNG for ICC/SC

- (T)RNG
 - How to get randomness in integrated circuit?
 - Analog circuits vs. metastability in bistable flip-flops
- PRNG – e.g. LCG (not secure!) or LFSR etc.
 - Based on hard number theoretic problems
 - Secure in cryptographic sense
 - Often use modular arithmetic
 - BBS, Micali-Schnorr, RSA PRNG ...
 - Based on common cryptographic functions
 - ANSI X9.17: 2-key 3DES
 - FIPS 186 and Yarrow-160: 2-key 3DES + SHA-1
 - Yarrow-160: in principle can be used AES + SHA-2

Password-based Public Key Cryptographic Techniques

- Based on using data with low entropy
 - Passwords, PINs ...
- Basic characteristics of these protocols
 - Mutual authentication
 - Establishment of high-quality key
 - Resistance to offline attacks
 - No additional persistent data needed
 - Still allows online attacks ☹
- Some practical applications
 - Remote authentication with Java Cards
 - New model of banking ATM networks
- Evolution of IEEE P1363.2

Conclusion

- HSM are very good for **user** authentication
- The security of current generation banking APIs is really bad with respect to **insider attacks**
- Number of standards implemented ensures **interoperability** but also **causes errors**
- High-quality **unpredictable** random numbers are very important in cryptography
- New methods allows generating of **high-quality** cryptographic material from **low-entropy** data
- My next research
 - Investigating (and improving) pseudorandom number generation and statistical testing
 - Password-based Public Key Cryptographic Techniques
 - Impact on user identification/authentication