Security Analysis and Vulnerabilities of TEGTSS-I Digital Signature Schemes

Beáta Nagy

Supervisors: Dr. János Tapolcai, Dr. Bence Ladóczki

May 30, 2024

Security of digital signature schemes

- Possible attacks:
  - Based on attacker's knowledge: key-only, known-message, chosen-message, **adaptively chosen-message attack**
  - Based on the goal: total break, forgery (universal, selective, **existential forgery**)
- $\rightarrow$ existential forgery against adaptively-chosen message attacks
- security proofs: computational hardness of mathematical problems, reduction
- e.g. Integer Factorization Problem, **Discrete Logarithm Problem**, Shortest Vector Problem, SAT Problem
  - DLP: finding x in the equation $g^x \equiv h \mod p$
- hash functions: one-way property

El Gamal Type Signature Schemes

- based on the algebraic properties of modular exponentiation and the discrete logarithm problem
- examples: **Schnorr**, DSA (US-standard), KCDSA (Korean-standard)
- idea: generalization of security proofs
- Trusted El Gamal Type Signature Scheme (TEGTSS)
  - two types, based on the use of the hash function
  - unforgeable relative to the DLP
  - use of the Random Oracle Model (ROM): hash functions are ideal random functions, programmable

Issues with ROM

- Non-existence in reality
- Programmability, observability
- Heuristic nature in security proofs $\rightarrow$ not applicable outside ROM
- Becomes vulnerable when replaced with actual hash functions

Modified Schnorr signatures

- Idea: construction of a vulnerable signature scheme, see if it fits the TEGTSS-I properties $\rightarrow$ vulnerability of the scheme
- Original Schnorr Signature Scheme:
  - signature: $s \equiv r + h(msg|R) \cdot x \mod q \rightarrow (s, R)$
  - verification: $g^s == R \oplus X^{h(msg|R)} \mod p$
- Modified Schnorr Signature Scheme:
  - hash only includes the message
  - signature: $s \equiv r + h(msg) \cdot x \mod q$

p, q: large primes, $q|p-1$
g: generator element of order q in $\mathbb{Z}_p^*$
s: signature, $S = g^s \mod p$
r: random element in $\mathbb{Z}_q^*$, $R = g^r \mod p$
$h = h(msg|R)$: hashed message in $\mathbb{Z}_q^*$
x: secret key in $\mathbb{Z}_q^*$, $X = g^x \mod p$

Modified Schnorr signatures

- Can be easily forged:
  - choosing s arbitrarily in $\mathbb{Z}_q^*$
  - computing $h(msg)$
  - computing $R = g^s \ominus X^{h(msg)} \mod p$
  - valid (s, R) pair without the knowledge of the secret key

Application on TEGTSS-I.

- Three functions are defined:
  - signature: $F_1() = s \mod q$
  - $R = g^{F_2()} \cdot X^{F_3()}$
  - $F_2() = s \mod q$
  - $F_3() = h \mod q$
- Additional hashing of nonce: $N = h_n(R)$
- Requirements:
  - $F_2(F_1()) + x \cdot F_3(F_1)) = r \mod q$ applies
  - if $h = h'$, then $F_3() = F_3'()$ applies by definition
  - one-to-one map between the values of h and N - does not apply
- Question: does one-to-one mapping change security results?

Security proof of TEGTSS-I

- *forking lemma*: if the attacker can construct a valid signature using a random oracle for hashing, then, the forking algorithm rewinds the attacker to a point before querying the random oracle $\rightarrow$ different RO response, two valid signatures for the same R $\rightarrow$ extraction of the secret key
- $s - s' = (h - h') \cdot x \mod q$
- Main theorem: if an attacker can find a valid signature for a new message with probability ϵ, then, with less than Q queries to the random oracle, with constant probability $1/96$, with less than $25Q/\epsilon$ replays of the attacker, with different random oracles, the secret key x will be extracted
  - extracting x implies solving the DLP $\rightarrow$ impossibility of probability ϵ of finding a valid signature

Security proof of TEGTSS-I on modified Schnorr

- proof is based on finding two distinct representations of $R \rightarrow$ F_2 or F_3 values have to differ
- forking lemma only applies to TEGTSS-I, intuition: applies here too (R depends on one less variable - the probability of finding one more verifying tuple with the same R does not decrease)
- one-to-one mapping in TEGTSS: used for proving that $F_3 = F_3'$ has vanishingly small probability given that $R = R' \rightarrow$ here $F_3() = h$, can only happen if $msg = msg' \rightarrow$ collision-resistance of message hash function, vanishingly small probability

Conclusion

- intuition: omitting the one-to-one map property of TEGTSS-I schemes does not change security results
- question of reducibility under ROM assumption to the DLP
- Future directions:
  - construct a more thorough argument of security problem with the ROM model
  - finding an instance that fits all the TEGTSS-I requirements, but is vulnerable in practice
  - investigation of other security proofs in the ROM model

References

Gianluca Dini (2023)
Digital Signatures: Types of Attacks and Security Considerations
Network Security 13–17.
Available at: http://docenti.ing.unipi.it/g.dini/Teaching/sanna/lecturenotes/applied-cryptography-digital-signature.pdf

Ernest Brickell, David Pointcheval, Serge Vaudenay, and Moti Yung (2001)
Design Validations for Discrete Logarithm Based Signature Schemes
PKC 2000 1751.
https://doi.org/10.1007/978-3-540-46588-1_19

Pascal Paillier and Damien Vergnaud (2005)
Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log
Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings 3788, 1–20.
https://iacr.org/archive/asiacrypt2005/001/001.pdf

Claus-Peter Schnorr (1989)
Efficient Identification and Signatures for Smart Cards
Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings 435, 239–252.
https://doi.org/10.1007/0-387-34805-0_22

David Pointcheval and Jacques Stern (2001)
Security Arguments for Digital Signatures and Blind Signatures
Journal of Cryptology 13.
https://doi.org/10.1007/s001450010003

Thank you for your attention!