Cryptanalysis and Improvement of the Smart–ID Signature Scheme

Augustin P. SARR

LACCA, UFR SAT, Université Gaston Berger de Saint–Louis, Saint–Louis, Senegal

Abstract. At ESORICS 2017, Buldas et al. proposed an efficient (software only) server supported signature scheme, geared to mobile devices, termed Smart–ID. A major component of their design is a clone detection mechanism, which allows a server to detect the existence of clones of a client’s private key share. We point out a flaw in this mechanism. We show that, under a realistic race condition, an attacker which holds a password camouflaged private share can launch an online dictionary attack such that (i) if all its password guesses are wrong, it is very likely that the attack will not be detected, and (ii) if one of its guesses is correct, it can generate signatures on messages of its choice, and the attack will not be detected. We propose an improvement of Smart–ID to thwart the attack we present.

Keywords: Smart–ID, four–prime RSA, mobile devices, clone detection, undetectable online dictionary attack.

1 Introduction

Digital signatures are used in every day communications and commerce. Given the widespread use of mobile devices, and the issue of a secure storage of the private keys, server supported software only solutions seem to be an interesting approach. Companies are now deploying software only threshold cryptography for key protection on mobile devices. Cyberetica [4] proposes an authentication and digital signature platform based on Smart–ID [1]. Smart–ID is a signature scheme, a modification of Damgård et al.‘s four prime RSA [2], geared to software only implementations on mobile devices.

A Smart–ID private key is shared between the device and a server, in a way to avoid the existence of a reference point for offline dictionary attacks, at both the device and the server. In addition, the signature generation integrates a clone detection mechanism which is claimed to allow the server to detect the existence of clones of a client’s private share. The number of Smart–ID users grew from 200,000 in 2017 [1] to 1,800,000 in 2019 [3].

Unfortunately, as we show in Section 2, there is a subtle flaw in the clone detection mechanism; this invalidates some of the claimed security attributes. Namely, we show that, under a plausible race condition, an attacker which holds a clone of the client’s password camouflaged private key share (recall that the
implementation is software-only) can issue up to \((T_0 - 1)\) undetectable password guesses, where \(T_0\) is the maximum wrong password guesses the service allows. Moreover, if one of the guesses is correct the attacker may generate signatures on messages of its choice, and this will \textit{not} be detected. We improve the clone detection mechanism to thwart the attack we present.

This paper is organized as follows. In Section 2 we recall the Smart–ID scheme, then we present an attack which invalidates the security of the clone detection mechanism. In Section 3, we propose an improved variant of Smart–ID, which thwarts the attack we present. We provide some concluding remarks in Section 4.

We use the following notations. If \(S\) is a set, \(a \leftarrow_n S\) means that \(a\) is chosen uniformly at random from \(S\). A prime number \(p\) is said to be \((l, s)\)-safe if \(p = 2ap_1 \cdots p_k\) where \(p'_i, i \in \{1, \ldots, k\}\) are primes greater than \(s\) and \(1 \leq a \leq l\). For an integer \(n\), \([n]\) denotes the set \(\{0, \ldots, n\}\). If \(n_1\) and \(n_2\) are such that \(\gcd(n_1, n_2) = 1\), \(\text{crt}((\sigma_1, n_1), (\sigma_2, n_2))\) refers to the unique \(\sigma \in [n_1n_1 - 1]\) such that \(\sigma = \sigma_1 \mod n_1\) and \(\sigma = \sigma_2 \mod n_2\).

## 2 Attacking the Smart–ID Signature Scheme

### 2.1 Description of the Scheme

Given a security parameter \(\eta\), the \texttt{Setup} algorithm defines an RSA modulus length \(k\), suitable values for \(l\) and \(s\), a public exponent \(e\), and a pseudorandom function \texttt{GenShare} which takes as inputs \(u \in \{0, 1\}^\eta\), a password \(\text{pwd} \in \{0, 1\}^l\) and an RSA modulus \(n_1\) and outputs \(d_1 < n_1\). It defines also a hash function \(H : \{0, 1\}^* \to \{0, 1\}^m\), with \(\eta_\ell \leq (k - 1)\), a padding scheme \(P\), and an upper bound \(T_0\) on the number of password attempts a user may perform.

\textit{Shared key generation.} Assuming a secure channel between the client \texttt{clt} and the server \texttt{srv}, \texttt{clt} generates two \((l, s)\)-safe primes \(p_1\) and \(q_1\) (such that \(\gcd(e, (p_1 - 1)(q_1 - 1)) = 1\)) and computes \(n_1 = p_1q_1\), and \(d_1 = e^{-1} \mod \phi(n_1)\). It generates \(u, r \leftarrow_n \{0, 1\}^\eta\) and \(d'_1 = \texttt{GenShare}(u, \text{pwd}, n_1)\), where \(\text{pwd}\) is the user’s password, and \(d''_1 = d_1 - d'_1 \mod \phi(n_1)\). Then, \texttt{clt} sends \(\langle d''_1, n_1, r \rangle\) to \texttt{srv}.

At receipt of \texttt{clt}’s message, \texttt{srv} generates two \((l, s)\)-safe primes \(p_2\) and \(q_2\) (such that \(\gcd(e, (p_2 - 1)(q_2 - 1)) = 1\)) and computes \(n_2 = p_2q_2\), \(d_2 = e^{-1} \mod \phi(n_2)\), and \(n = n_1n_2\). Then, it sends back \(n\) to \texttt{clt} and stores \(\langle n, n_1, n_2, d''_1, d_2, r, T = T_0\rangle\). At receipt of \texttt{srv}’s message, \texttt{clt} stores \(\langle n, n_1, u, r \rangle\) and safely deletes all the other values. The public key is \(pk = (e, n)\).

\textit{Signature Generation.} For a signature on \(m' \in \{0, 1\}^*\), \texttt{clt} computes \(m = P(H(m'))\); then, from the user’s password \(\text{pwd}\), it derives \(d'_1 = \texttt{GenShare}(u, \text{pwd}, n_1)\) and \(y = m^{d'_1} \mod n_1\). It chooses \(r' \leftarrow_n \{0, 1\}^\eta\) and sends \(\langle y, m, r, r'\rangle\) to \texttt{srv}.

At receipt of \(\langle y, m, r, r'\rangle\), \texttt{srv} verifies that \texttt{clt} is active; if so, it lookups the record \(\langle n_1, n_2, d''_1, d_2, r, T\rangle\). If \(r \neq r\), \texttt{srv} deactivates \texttt{clt}; else, it computes \(\sigma_1 = ym^{d''_1} \mod n_1\) and \(\hat{m} = \sigma_1^e \mod n_1\). If \(\hat{m} \neq m\), it drops the request,
decrements $T$, and deactivates $\text{clt}$ in the case $T = 0$. If $\hat{m} = m$, it computes $\sigma_2 = m^{d_2} \mod n_2$, $\sigma = \text{crt}((\sigma_1, n_1), (\sigma_2, n_2))$, sends back $\langle \sigma, m \rangle$ to $\text{clt}$, sets $T = T_0$, and stores $\langle n_1, n_2, d_1', d_2, r', T \rangle$. At receipt of $\langle \sigma, m \rangle$, $\text{clt}$ stores $\langle n, n_1, u, r' \rangle$. The signature on $m'$ is $\sigma$.

**Signature Verification.** To verify a signature $\sigma$ on $m'$, with regard to a public key $pk = (n, e)$, one computes $m = P(H(m'))$ and verifies that $\sigma^e = m \mod n$.

**The Clone Detection Mechanism.** A major component in Smart–ID’s design is its clone detection mechanism. During the key pair generation the client $\text{clt}$ sends to the server not only a share $d_1''$ of $d_1$, the part of the private key it generates, but also a nonce $r$ the server should expect to receive in $\text{clt}$’s next service query. And, each time $\text{clt}$ uses the services, it sends a new nonce $r'$ together with $r$; from there $\text{srv}$ expects to receive $r'$ in $\text{clt}$’s next query. An adversary $\mathcal{A}$ which holds a clone of $\text{clt}$’s private share $d_1$ has to send a new nonce $r'$ at each service query. Then, it is expected that the value $\mathcal{A}$ sends be different from the value $r$ at the legitimate client $\text{clt}$. And then, the existence of the clone be detected when $\text{clt}$ attempts to query the service.

Unfortunately, this analysis mistakenly assumes that an attacker which holds a clone of $\text{clt}$’s private share (which may password camouflaged or not) will follow the protocol’s description. In particular, the analysis assumes that $\mathcal{A}$ will choose $r'$ uniformly at random from $\{0,1\}^\eta$. As we show, this seemingly insignificant shortcoming induces major weaknesses in the clone detection mechanism.

### 2.2 Undetectable Online Password Guesses

Assuming a realistic race condition, we show how an attacker $\mathcal{A}$ which holds a clone of $\text{clt}$’s password camouflaged private share, and aims to have valid signatures on $m'_1, m'_2, \ldots, m'_k \in \{0,1\}^*$, can issue up to $(T_0 - 1)$ online password guesses such that (i) if all the guesses are wrong, it is very likely that the attack remains undetected, and (ii) if one of the guesses is correct, $\mathcal{A}$ generates signatures on the messages and the attack will not be detected. Clearly, this indicates a failure of Smart–ID’s clone detection mechanism.

We assume that $\mathcal{A}$ obtains a clone of a client’s password camouflaged share after a successful use of the service, so that $T = T_0$ at $\text{srv}$; $\mathcal{A}$ performs as in Algorithm 1.

Under the realistic assumption that the legitimate client $\text{clt}$ does not use the service before the attack is completely executed, it is very likely that the attack remains undetected. In effect, $\mathcal{A}$ performs at most $(T_0 - 1)$ password guesses. And, if none of the guesses is correct, the device is not deactivated ($T = 1$, there remains one possible attempt). Now, as the attacker always used $r' = r$ as a next incoming nonce, the server still expects to receive a nonce with value $r$ in the next request. This corresponds the nonce value at $\text{clt}$. So, it is very likely that when the legitimate device owner connects to the service, it derives the right private share $d_1'$ and sends the nonce $r$, so that the value of $T$ is set again to $T_0$. 
Algorithm 1 Undetectable online password guesses

1) Computes \( m_1 = \mathcal{P}(H(m'_1)) \), and recover the tuple \( \langle n, n_1, u, r \rangle \) (which is stored unencrypted in the clone);
2) For each password \( pwd_i \), \( i \in \{1, \cdots, T_0 - 1\} \), to test, do the following:
   a) Compute \( d'_i = \text{GenShare}(u, pwd_i, n_1) \) and \( y_{1,i} = m_1^{d'_i} \mod n_1 \);
   b) Send \( \langle y_{1,i}, m_{1,i}, r, r \rangle \) to \( \text{srv} \);
   c) If \( \text{srv} \) responds with a pair \( \langle \sigma_1, m_1 \rangle \) such that \( \sigma_1^r = m_1 \mod n \) then
      i) Store \( pwd = pwd_i \) and \( d'_i = \text{GenShare}(u, pwd_i, n_1) \) as the right password and private key share, respectively;
      ii) For each \( m_j = \mathcal{P}(H(m'_j)), j \in \{2, \cdots, k\} \):
          a) Compute \( y_{j} = m_j^{d'_j} \mod n_1 \) and send \( \langle y_{j}, m_j, r, r \rangle \) to \( \text{srv} \);
          b) At receipt of \( \langle \sigma_j, m_j \rangle \), store \( \sigma_j \) as a signature on \( m'_j \).

and the attacker’s wrong password guesses remain undetected. In contrast, if the device owner mistakenly types a wrong password, the device is deactivated and the attack is detected. This event can be made rarer by reducing the number of password guesses the attacker performs (to \( (T_0 - 2) \), for instance).

If one of the password guesses is correct, \( \mathcal{A} \) which is now aware of \( d'_i \) generates the signatures \( \sigma_j \) on \( m'_j \) for \( j \in \{1, \cdots, k\} \). After the signature generations, the value of \( T \) at \( \text{srv} \) is \( T_0 \), and the value of \( r \) \( \text{srv} \) expects to receive is the one at \( \text{clt} \). Hence, under the race condition that \( \text{clt} \) does not use the service before the attack is completely executed, the attack will not be detected.

3 Improving the Smart–ID Scheme

We propose a variant of Smart–ID, which resists to our attack.

At first glance, it may be tempting to modify the server to require that two consecutive nonces be different, i. e., in a signature generation, the current nonces \( r \) and the next nonce \( r' \) a client provides be different. This modification is not enough, if \( (T_0 - 1) \geq 3 \) or if one of the password guesses is correct, as the attacker can use consecutive nonces \( r = r_1, r_2, \cdots, r_L \), with \( L \geq (T_0 - 1) \) \( (L = T_0 - 1 \) if all the guesses are wrong) such that \( r_1 \neq r_2, r_2 \neq r_3, \cdots, \) but \( r_L = r \).

More generally, the server can require that consecutive \( T_0 \) nonces be pairwise different; this requirement induces no modification at the client (the probability of collision \( \leq T_0^2 / 2^n \), which is negligible). Unfortunately, this change remains unsatisfactory, as if \( \mathcal{A} \) succeeds in one of its guesses, it can query the service \( L > T_0 \) times, with nonces \( r = r_1, r_2, \cdots, r_k \) such that \( r_1 \neq r_2, r_2 \neq r_3, \cdots, \) but \( r_L = r \). The attack will not be detected.

A better approach is to modify the server so that it contributes to the nonce generation. In this way, it becomes infeasible for a malicious client to masquerade so that the nonce \( \text{srv} \) expects to receive holds a specific value. We describe hereunder the modified Smart–ID variant we obtain with such a modification. The setup and signature verification algorithms are the same as in original scheme.
Shared key generation. We assume a secure channel between the client clt and
the server srv. The client generates two \((l, s)\)-safe primes \(p_1\) and \(q_1\) and computes
\(n_1 = p_1q_1\) and \(d_1 = e^{-1} \mod \phi(n_1)\). It generates \(u, r_c \leftarrow \{0, 1\}^\nu\) and computes
\(d'_1 = \text{GenShare}(u, \text{pwd}, n_1)\), where \(\text{pwd}\) is the user’s password, and \(d''_1 = d_1 - d'_1\)
\(\mod \phi(n_1)\). Then it sends \((d''_1, n_1, r_c)\) to \(\text{srv}\).

At receipt of \(\text{clt}\)’s message, \(\text{srv}\) generates two \((l, s)\)-safe primes \(p_2\) and \(q_2\); it
computes \(n_2 = p_2q_2\), \(d_2 = e^{-1} \mod \phi(n_2)\), \(r_s \leftarrow \{0, 1\}^\nu\), and \(n = n_1n_2\). Then,
it sends back \((n, r_s)\) to \(\text{clt}\) and stores \((n_1, n_2, d'_1, d_2, r_c, r_s, T = T_0)\). At receipt of \(\text{srv}\)’s message, \(\text{clt}\) stores \(\langle n, n_1, u, r_c, r_s \rangle\) and safely deletes all the other values.
The public key is \(pk = (e, n)\).

Signature Generation. For a signature on \(m'\), \(\text{clt}\) generates \(m = \text{P(H(m'))}\).
Then, it gets the user’s password \(\text{pwd}\), and derives \(d'_1 = \text{GenShare}(u, \text{pwd}, n_1)\)
and \(y = m^{d'_1} \mod n_1\). It chooses \(r_c' \leftarrow \{0, 1\}^\nu\) and sends \((y, m, r_c, r_s, r_c')\) to \(\text{srv}\).

At receipt of \((y, m, r_c, r_s, r_c')\), \(\text{srv}\) verifies that \(\text{clt}\) is active. If so, it lookups
the record \(\langle n_1, n_2, d'_1, d_2, r_c', r_s, T \rangle\). It computes \(\sigma_1 = ym^{d_c''} \mod n_1\) and \(\hat{m} = \sigma_1^r\)
\(\mod n_1\), and performs as follows.

- If \((\hat{r}_c, \hat{r}_s) \neq (r_c, r_s)\) and \(\hat{m} \neq m\) then \(\text{srv}\) alerts\(^1\) on the existence of a clone
of the password camouflaged share of \(\text{clt}\), and drops the request.
- If \((\hat{r}_c, \hat{r}_s) \neq (r_c, r_s)\) and \(\hat{m} = m\) then \(\text{clt}\) deactivated the client (there is
probably a clone of \(\text{clt}\)’s private share).
- If \((\hat{r}_c, \hat{r}_s) = (r_c, r_s)\) and \(\hat{m} \neq m\) then
  - \(\text{srv}\) chooses \(r'_c \leftarrow \{0, 1\}^\nu\), and sends \("0", r'_c\) to \(\text{clt}\);
  - it decrements \(T\), stores \(\langle n_1, n_2, d'_1, d_2, r'_c, T \rangle\), and deactivates \(\text{clt}\) in the
case \(T = 0\).
- If \((\hat{r}_c, \hat{r}_s) = (r_c, r_s)\) and \(\hat{m} = m\) then \(\text{srv}\) computes \(\sigma_2 = m^{d_2} \mod n_2\),
\(\sigma = \text{clt}(\langle \sigma_1, n_1 \rangle, \langle \sigma_2, n_2 \rangle)\), chooses \(r'_s \leftarrow \{0, 1\}^\nu\), and sends back \(\langle \sigma, m, r'_s \rangle\)
to \(\text{clt}\). It sets \(T = T_0\) and stores \(\langle n_1, n_2, d'_1, d_2, r'_c, r'_s, T \rangle\).

At receipt of \(\text{srv}\)’s message, \(\text{clt}\) performs as follows.

- If the message parses as \("0", r'_s\) then \(\text{clt}\) stores \(\langle n, n_1, u, r'_c, r'_s \rangle\) (the user
probably typed a wrong password and the signature generation failed).
- Else (the message parses as \(\langle \sigma, m, r'_s \rangle\)),
  - \(\text{clt}\) stores \(\langle n, n_1, u, r'_c, r'_s \rangle\);
  - the signature on \(m'\) is \(\sigma\).

Clone Detection. By defining the nonce a client provides, when using the service,
as a pair \((r_c, r_s)\) such that \(r_c\) is generated by the client and \(r_s\) by the server,
neither the server nor the client can masquerade so that a nonce takes a specific
value. In this way, once an attacker (which holds either a clone of the password
camouflaged share or a clone of \(\text{clt}\)’s private share) uses the service, through an
online password guess or a signature generation, the nonce the server expects
for the next query changes. And, except with negligible probability, it becomes
different from the one at \(\text{clt}\). Thereby, the existence of the clone will be detected
the next time \(\text{clt}\) uses the service.

\(^1\) There may exist a secondary channel between \(\text{srv}\) and \(\text{clt}\).
Remark 1. a) The clone detection mechanism may be of interest in other client–server settings.
b) To reduce the communication cost of a signature generation, the nonce $clt$ sends can be defined to be $H'(r_c, r_s)$, for some cryptographic hash function $H': \{0, 1\}^* \to \{0, 1\}^\eta$, instead of $(r_c, r_s)$.

4 Concluding Remarks

The Smart–ID scheme, built from Damgård et al.’s four prime RSA, is geared to server supported software only implementations on mobile devices. While this approach provides an interesting solution for the issue of a secure storage of the private keys on mobile devices, it yields easily clonable (software only) applications. To mitigate this issue, the Smart–ID design integrates a clone detection mechanism.

We pointed out a subtle shortcoming in the clone detection mechanism and showed, under a realistic race condition, how an attacker which holds a clone of the password camouflaged private share of a client can launch online password guesses such that (i) if all the guesses are wrong, it is likely that the attack will not be detected, and (ii) if one of the guesses is correct, the attacker may generate signatures on messages of its choice, while the attack will not be detected. We proposed a variant of Smart–ID which resists the attack we present.

It would be a nice feature of the Smart–ID scheme if device owners had the possibility to update their passwords. In a forthcoming stage, we will explore the question of password updates in password–based server supported signature schemes.

References