Cryptography and Security of Digital Devices

Exam Code: 095947 (old 090959), A.Y. 2019–2020, Semester: 2

Prof. G. Pelosi

February 18th, 2020 – Exam Session

Name: ..... Surname: .....

Signature: ..... Student ID: .....

Time: 2h:15'. Use of textbooks, notes, internet connected laptops (or any other devices) and of software tools is not allowed. Pencil writing is allowed.
Write your name on any additional sheet and sign it.

Question 1 [2 pts]
An X.509 certificate for `foo.com` includes the 256 bit RSA public key for the aforementioned common name, and its MD5 hash signed with 512 bit RSA by Faust Certification Authority inc. Alice's browser contains a valid, trusted root CA certificate for Faust CA inc.

(a) Highlight which are Alice's concerns (all of them) toward the security of a possible TLS communication with foo.com, instantiated with the aforementioned X.509 certificate.

Solution:

The first issue regarding the certificate is an insufficient keylength choice for both the RSA algorithms; anything below 2048 bit is to be considered insecure for RSA. The second concern is the fact that it is possible to find almost-arbitrary collisions to MD5 (i.e. the message is picked arbitrarily, save for the last MD5 block), which in turn allows to forge a certificate having the same signature as the one of foo.com even without passing by the CA.

Question 2 [6 pts]
Rosen Association inc. mandates the use of encrypted disk volumes for its own employees enforcing the following:

- All the disks have two partitions, one containing the OS binaries (with a non-integrity checking filesystem), while the other hosts the employee data. The OS partition is to be encrypted with AES-256-CBC with a randomized IV when the partition is created, while the user data partition (i.e., the employee partition) should employ AES-256-CTR, using the string "NEXUS6-ROSENInc." as IV.
- All the employee partitions are set up by the system administrator which, during formatting, takes care to fill the space within the encrypted volume with zeroes, so to fill the effective physical diskspace with random data.

- The employees are enforced to pick their disk encryption passwords as 16 character random strings containing decimal digits. The password is hashed through SHA-2-256 to fill in the AES-256 key.

(a) Discuss the choices of Rosen inc. concerning the choice of the encryption algorithm for the OS partition, highlighting issues and proposing a way to fix them.

(b) Discuss the choice of the encryption algorithm for the employee partition, and the decision of the system adminstrator to wipe the internal space of the disk volume.

(c) Discuss the password policy chosen by Rosen, providing a quantitative estimate for the attacker effort to be spent to completely break the whole system, in the most efficient way possible

Solution:

(a) Picking a block cipher in CBC mode, without any integrity check, allows an attacker to exploit the CBC malleability to his own advantage. In particular, considering the case of a disk volume where an OS is stored, it is possible to alter partially the OS binaries without deciphering the volume.

(b) The choice of a counter-mode of operation for disk encryption is not problematic as long as the CTR IV is picked at random. Given the choice of Rosen inc. to employ a fixed IV, the pseudorandom keystream obtained out of the AES-256 in CTR mode is the same for all the partitions of the employees using the same password. This in turn allows to extract information without the secret key, adding via `xor` two instances of encrypted data with the same password (e.g. two full disk dumps taken in different moments).

The decision of the system administrators to fill with zeroes the partitions effectively worsens the issue: the attacker is basically provided with the whole keystream, if he is able to dump the disk of a laptop right after it has been issued.

(c) Considering the password policy, the effective password space is 10^{16}, which is equivalent to roughly 2^{53}. This in turn implies that a full exhaustive search for the password is within feasibility for moderately motivated attackers. As a further issue, the passwords are used as-is, without any salted hashing scheme, thus allowing an attacker to successfully exploit TMTO strategies.

Question 3 [2 pts]

A company is employing keyed RIPEMD-64 hashes (64-bit digest) as an integrity checking mechanism for files on a disk. The security officer is currently concerned with the security margin against intentional replacement of files with garbage data and suggests to change the keyed hashing mechanism to SHA-2-256. The commercial department points out that employing SHA-2-256 would increment the amount of required disk space and, to reduce the migration costs, proposes to employ SHA-2-256 to hash the file contents, and store only the first quarter of the digest for integrity checking.

(a) Is the security officer concern well justified? Provide a quantitative motivation to it.

(b) Is it possible to adopt the commercial department solution? Justify quantitatively the answer.

Solution:

(a) Yes: if somene knows the key, a 64 bit hash implies the possibility of obtaining a collision through exhaustive search in around 2^{32} operations, thus the intentional replacement of files with garbage data is well within the realm of feasibility.

(b) No: performing the comparison only on the first 64 bits of the digest of SHA-2-256, and assuming that the bits of the first quarter of the hash follow the same uniform distribution as the rest of it, it is possible to obtain a partially colliding digest with the same computational effort of the previous hashing mechanism.

Question 4 [4 pts]
Consider the finite field $\mathbb{F}_{2^6}$.

(a) Show the number of irreducible polynomials that can be used to represent the field elements.

(b) Show the number of primitive polynomials that can be used to represent the field elements.

(c) Verify that $f(x)=x^6+x+1$ is a primitive polynomial.

Solution:

(a) $2^6 = 1 \cdot N_1(2) + 2 \cdot N_2(2) + 2 \cdot N_3(2) + 6 \cdot N_6(2) \Leftrightarrow$
$2^6 = 1 \cdot 2 + 2 \cdot \frac{2^2-2}{2} + 2 \cdot \frac{2^3-2}{3} + 6 \cdot N_6(2) \Rightarrow$
$N_6(2) = \frac{2^6-2-2-4}{6} = 9.$

(b) $M_6(2) = \frac{\varphi(|\mathbb{F}_{2^6}|)}{6} = \frac{\varphi(63)}{6} = \frac{(3^2-3)\cdot(7-1)}{6} = 6.$

(c) $f(x)$ is primitive if its roots are generators of the multiplicative group $\left(\mathbb{F}^*_{2^6}, \cdot\right)$.
Remember that $\mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/\langle f(x)\rangle \cong \mathbb{F}_2(\alpha)$, where $\alpha \notin \mathbb{F}_2$, $f(\alpha)=0$ and the elements of the field can be represented as $\mathbb{F}_2(\alpha)=\{\theta_5\alpha^5 + \ldots + \theta_1\alpha + \theta_0\}$, $\theta_i \in \{0,1\}$, $0 \leq i \leq 5$.
Therefore, $f(x)$ is primitive over $\mathbb{F}_{2^6}$, $n=|\mathbb{F}_{2^6}|=63=3^2\cdot 7$,
iif assuming $f(\alpha)=0 \Leftrightarrow \alpha^6 \equiv \alpha+1$, the following relations hold

$$\begin{cases} \alpha^3 \stackrel{?}{\not\equiv} 1 \\ \alpha^7 \stackrel{?}{\not\equiv} 1 \\ \alpha^9 \stackrel{?}{\not\equiv} 1 \\ \alpha^{21} \stackrel{?}{\not\equiv} 1 \\ \alpha^{63} \stackrel{?}{\equiv} 1 \end{cases} \Rightarrow \begin{cases} \alpha^3 \not\equiv 1 \\ \alpha^7 \equiv \alpha^6 \cdot \alpha \equiv \alpha^2 + \alpha \not\equiv 1 \\ \alpha^9 \equiv \alpha^7 \cdot \alpha^2 \equiv \alpha^4 + \alpha^3 \not\equiv 1 \\ \alpha^{21} \equiv (\alpha^7)^3 \equiv (\alpha \cdot (\alpha+1))^3 \equiv \ldots \equiv \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1 \not\equiv 1 \\ \alpha^{63} \equiv \ldots \equiv 1 \text{ ok!} \end{cases}$$

Question 5 [6 pts]
Consider the following relation: $11 \equiv 2^x \bmod 13$.

(a) Compute the discrete logarithm $x \equiv_{\varphi(13)} \log_2^{\mathrm{D}} 11$ applying the Pohlig-Hellman method.

(b) Show the computational complexity of the Pohlig-Hellman algorithm. When is it appropriate to use this method?

Solution:

(a) We are considering the algebra of the group $(\mathbb{Z}_{13}^*, \cdot)$,
with $|\mathbb{Z}_{13}|=\varphi(13)=12=2^2\cdot 3$ elements.

$$x \equiv_{\varphi(13)} \log_2^{\mathrm{D}} 11 \quad \Leftrightarrow \quad \begin{cases} x \equiv x_1 \bmod 2^2 \\ x \equiv x_2 \bmod 3 \end{cases} \quad \Rightarrow$$

$$x \equiv_{12} x_1 \cdot 3 \cdot (3^{-1} \bmod 4) + x_2 \cdot 4 \cdot (4^{-1} \bmod 3) \Rightarrow x \equiv_{12} 9x_1 + 4x_2$$

The Pohlig-Hellman algorithm compute $(x_1 \bmod p_1^2)$, with p_1=2, as follows:
let the 2-radix expansion of $x_1 \bmod 2^2$ be $x_1 = l_0 + l_1 2$ and denote as: g=2 the base of the logarithm, β=11, n=12 the order of the group
$\eta = g^{\frac{n}{p_1}} \equiv_{13} 2^6 \equiv_{13} 12$
$\gamma_0 = 1$, $\delta_0 \equiv (\beta\gamma_0^{-1})^{\frac{n}{p_1}} \equiv_{13} 11^6 \equiv_{13} 12$.
Knowing that $\delta_0 = (g^x\gamma_0^{-1})^{\frac{n}{p_1}} \equiv g^{x_1\frac{n}{p_1}} \Rightarrow \delta_0 \equiv (g^{\frac{n}{p_1}})^{l_0}$, we have
$\delta_0 \equiv_{13} \eta^{l_0} \Leftrightarrow 12 \equiv_{13} 12^{l_0}$, therefore: $l_0 = 1$.
$\gamma_1 = \gamma_0 \cdot g^{l_0 p_1^0} \equiv_{13} 2$, $\delta_1 \equiv (\beta\gamma_1^{-1})^{\frac{n}{p_1^2}} \equiv_{13} (11 \cdot 2^{-1})^3 \equiv_{13} (11 \cdot 7)^3 \equiv_{13} 12$.
Knowing that $\delta_1 = (g^x\gamma_1^{-1})^{\frac{n}{p_1^2}} \equiv (g^{x_1-l_0})^{\frac{n}{p_1^2}} \Rightarrow \delta_1 \equiv (g^{\frac{n}{p_1}})^{l_1}$, we have
$12 \equiv_{13} \eta^{l_1} \Leftrightarrow 12 \equiv_{13} 12^{l_1}$, therefore: $l_1 = 1$.
$x_1 = 1 + 1 \cdot 2 = 3$.

The Pohlig-Hellman algorithm compute $(x_2 \bmod p_2^1)$, with p_2=3, as follows:
let the 3-radix expansion of $x_2 \bmod 3$ be $x_2 = l_0$ and denote as: g=2 the base of the logarithm, β=11, n=12 the order of the group
$\eta = g^{\frac{n}{p_2}} \equiv_{13} 2^4 \equiv_{13} 3$
$\gamma_0 = 1$, $\delta_0 \equiv (\beta\gamma_0^{-1})^{\frac{n}{p_2}} \equiv_{13} 11^4 \equiv_{13} 3$.
from $\delta_0 \equiv (g^{\frac{n}{p_2}})^{l_0}$, we have
$\delta_0 \equiv_{13} \eta^{l_0} \Leftrightarrow 3 \equiv_{13} 3^{l_0}$, therefore: $l_0 = 1$.
$x_2 = 1$.

$x \equiv_{12} 9x_1 + 4x_2 \equiv_{12} 27 + 4 \equiv_{12} 7$.

Validation: $2^x \stackrel{?}{\equiv}_{13} 11$, taking x=7, it is true that $2^7 \equiv_{13} 11$.

(b) (see lectures...)

Question 6 [12 pts]

(a) Consider the RSA modulus $n = p \cdot q = 713 = 23 \cdot 31$

- Apply the Miller-Rabin primality test to the factor p employing as bases $a = 3$, $b = 7$.
- Given the public exponent e=7 $\in \mathbb{Z}_{\varphi(n)}^*$, show the value of the RSA private key, k_{priv}=$(p, q, \varphi(n), d)$ and specify every step of the computation.

- Apply a Right-to-Left Square & Multiply strategy to compute the ciphertext $c_1 = m^{13} \bmod n$, with $m = 101 \bmod n$ employing a radix-2 encoding of the exponent, and apply a Left-to-Right Square & Multiply strategy to re-compute the same value employing a radix-4 encoding of the exponent.

(b) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times),\ p = 23$

- Show the working principle of the Montgomery Multiplication and the smallest admissible value for the Montgomery Radix: R
- Exhibit the values R', p' that satisfy the relation: $\gcd(R, p) = R\,R' - p\,p' = 1$, justifying the procedure
- Compute the Montgomery multiplication $\widetilde{C} = \text{MonPro}(\widetilde{A}, \widetilde{B}) = \widetilde{A} \times \widetilde{B} \times R^{-1} \bmod p$, where $\widetilde{A} = 16_{\text{dec}}$ and $\widetilde{B} = 11_{\text{dec}}$, assuming a binary encoding of the operands.

Solution:
(Sketch)

(a) $\varphi(n) = 22 \cdot 30 = 2^2 \cdot 3 \cdot 5 \cdot 11 = 660$,
$d = e^{\varphi(\varphi(n))-1} \bmod \varphi(n) = 7^{159} \bmod 660 = 283$.

Right-to-Left S&M:
$c_1 \equiv_n m^{13_{\text{dec}}} \equiv_{713} 101^{\langle 1101 \rangle_2} \equiv_{713} (101^{2^3})^1 \cdot (101^{2^2})^1 \cdot (101^{2^1})^0 \cdot (101^{2^0})^1 \equiv_{713} \ldots$
$\equiv_{713} 357$.
To apply the Left-to-Right S&M with a 4-radix expansion of the exponent it is convenient to be able to compute the 4-th power of an integer modulo 713, efficiently;
in addition, we need to pre-compute: $m \equiv_{713} 101$, $m^2 \equiv_{713} 219$, $m^3 \equiv_{713} 16$. Thus,
$c_1 \equiv_n m^{13_{\text{dec}}} \equiv_{713} 101^{\langle 31 \rangle_4} \equiv_{713} (101^3)^4 \cdot 101 \equiv_{713} \ldots \equiv_{713} 357$.

(b) $R = 2^5 = 32$. $\gcd(32, 23) = 32(-5) - 23(-7) = 1 \Rightarrow$
$R' = R^{-1} \bmod p \equiv_{23} -5 \equiv_{23} 18$, $p' = p^{-1} \bmod R \equiv_{32} -7 \equiv_{32} 25$.

$p = 23_{\text{dec}} = \langle 10111 \rangle_2, \qquad p'_0 = (p' \bmod 2) = 1$
$\widetilde{B} = 11_{\text{dec}} = \langle \widetilde{B}_4 \widetilde{B}_3 \widetilde{B}_2 \widetilde{B}_1 \widetilde{B}_0 \rangle_2 = \langle 01011 \rangle_2$
$\widetilde{A} = 16_{\text{dec}} = \langle \widetilde{A}_4 \widetilde{A}_3 \widetilde{A}_2 \widetilde{A}_1 \widetilde{A}_0 \rangle_2 = \langle 10000 \rangle_2$

00000	+
00000	$\widetilde{A}_0 \widetilde{B} = \langle 00000 \rangle_2$
00000	+
00000	$(p'_0 x_0)\, p = \langle 00000 \rangle_2$
00000	perform a right-shift of 1 bit
$\vdots$	$\vdots$
00000	+
01011	$\widetilde{A}_4 \widetilde{B} = \langle 01011 \rangle_2$
01011	+
10111	$(p'_0 x_0)\, p = \langle 10111 \rangle_2$
100010	perform a right-shift of 1 bit
10001	

$\widetilde{C} = \langle 10001 \rangle_2 = 17_{\text{dec}} <$ **p**, Thus: $C \equiv_p \mathsf{MonPro}(16_{\text{dec}}, 11\text{dec}) \equiv_{23} 17_{\text{dec}}$

Validation:

$\widetilde{C} = \mathsf{MonPro}(16, 11) \stackrel{\text{def}}{=} 16 \cdot 11 \cdot R^{-1} \bmod p \equiv_{23} 15 \cdot 32^{-1} \equiv_{23} 15 \cdot 18 \equiv_{23} 17_{\text{dec}}$