Cryptographic protocols

Myrto Arapinis
School of Informatics
University of Edinburgh

March 14, 2016
Applications exchanging sensitive data over a public network:

- eBanking,
- eCommerce,
- eVoting,
- ePassports,
- Mobile phones,
- ...
Applications exchanging *sensitive data* over a *public network*:

- eBanking,
- eCommerce,
- eVoting,
- ePassports,
- Mobile phones,
- ... 

A malicious agent can:

- record, alter, delete, insert, redirect, reorder, and reuse past or current messages, and inject new messages

  \[\rightarrow\text{the network is the attacker}\]

- control dishonest participants
More complex systems needed...
More complex systems needed...

\[ e = E(K_E, \text{Transfer 100 € on Amazon's account}) \]

\[ m = MAC(K_M, E(K_E, \text{Transfer 100 € on Amazon's account})) \]
More complex systems needed...

\[ e = E(K_E, \text{Transfer 100 € on Amazon's account}) \]
\[ m = MAC(K_M, E(K_E, \text{Transfer 100 € on Amazon's account})) \]

Replay attack

\[ (e, m) \rightarrow \]

\[ (e, m) \rightarrow \]

\[ (e, m) \rightarrow \]
Confidentiality: Some information should never be revealed to unauthorised entities.

Integrity: Data should not be altered in an unauthorised manner since the time it was created, transmitted or stored by an authorised source.

Authentication: Ability to know with certainty the identity of a communicating entity.

Anonymity: The identity of the author of an action (e.g. sending a message) should not be revealed.

Unlinkability: An attacker should not be able to deduce whether different services are delivered to the same user

Non-repudiation: The author of an action should not be able to deny having triggered this action.
Cryptographic protocols

Programs relying on cryptographic primitives and whose goal is the establishment of “secure” communications.
Cryptographic protocols

Programs relying on cryptographic primitives and whose goal is the establishment of “secure” communications.

But!

Many exploitable errors are due not to design errors in the primitives, but to the way they are used, i.e. bad protocol design and buggy or not careful enough implementation.
Numerous deployed protocols are flawed!!!

Needham-Schroeder protocol - G. Lowe, ”An attack on the Needham-Schroeder public-key authentication protocol”

Kerberos protocol - I. Cervesato, A. D. Jaggard, A. Scedrov, J. Tsay, and C. Walstad, ”Breaking and fixing public-key kerberos”


PKCS#11 API - M. Bortolozzo, M. Centenaro, R. Focardi, and G. Steel, ”Attacking and fixing PKCS#11 security tokens”

BAC protocol - T. Chothia, and V. Smirnov, ”A traceability attack against e-passports”

AKA protocol - M. Arapinis, L. Mancini, E. Ritter, and M. Ryan, ”New privacy issues in mobile telephony: fix and verification”
Logical attacks

Many of these attacks do not even break the crypto primitives!!
Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\left\{ \left\{ m \right\}^k_1 \right\}^k_2 = \left\{ \left\{ m \right\}^k_2 \right\}^k_1$$

where $\{m\}_k$ denotes the encryption of message $m$ under the key $k$

Example: RSA
Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\{\{m\}_k\}_k = \{\{m\}_k\}_k$$

where \(\{m\}_k\) denotes the encryption of message \(m\) under the key \(k\)

Example: RSA

\[\begin{array}{c|c}
A & B \\
\hline \\
\end{array}\]
Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\{\{m\}_k\}_k = \{\{m\}_k\}_k$$

where $$\{m\}_k$$ denotes the encryption of message $$m$$ under the key $$k$$

Example: RSA
Example of a logical attack

Assume a commutative symmetric encryption scheme

\[
\{\{m\}_{k_1}\}_{k_2} = \{\{m\}_{k_2}\}_{k_1}
\]

where \(\{m\}_k\) denotes the encryption of message \(m\) under the key \(k\)

Example: RSA
Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\{\{m\}^k_1\}^k_2 = \{\{m\}^k_2\}^k_1$$

where $\{m\}^k$ denotes the encryption of message $m$ under the key $k$

Example: RSA

since $\{\{\text{pin: 3443}\}^{pk_A}_{pk_B}\}^{pk_B} = \{\{\text{pin: 3443}\}^{pk_B}_{pk_A}\}^{pk_A}$ by commutativity
Example of a logical attack

Assume a commutative symmetric encryption scheme

\[ \text{\\{\\{m\\}k_1\}}k_2 = \text{\\{\\{m\\}k_2\}}k_1 \]

where \( \text{\\{m\\}k} \) denotes the encryption of message \( m \) under the key \( k \)

Example: RSA

No authentication!

since \( \text{\\{\\{\text{pin: 3443}\\}pk_A\}}pk_B = \text{\\{\\{\text{pin: 3443}\\}pk_B\}}pk_A \) by commutativity
Example of a logical attack

Assume a commutative symmetric encryption scheme

\[ \{\{m\}^k_1\}^k_2 = \{\{m\}^k_2\}^k_1 \]

where \(\{m\}_k\) denotes the encryption of message \(m\) under the key \(k\)

Example: RSA

No authentication!

since \(\{\{\text{pin: 3443}\}^{pk_A}^{pk_B}\} = \{\{\text{pin: 3443}\}^{pk_B}^{pk_A}\}\) by commutativity
Example of a logical attack

Assume a commutative symmetric encryption scheme

\( \{ \{ m \}^k_1 \}^k_2 = \{ \{ m \}^k_2 \}^k_1 \)

where \( \{ m \}^k \) denotes the encryption of message \( m \) under the key \( k \)

Example: RSA

No authentication!

since \( \{ \{ \text{pin: 3443} \}^{pk_A}_{pk_B} \}^{pk_B}_{pk_A} = \{ \{ \text{pin: 3443} \}^{pk_B}_{pk_A} \}^{pk_A}_{pk_B} \) by commutativity
Example of a logical attack

Assume a commutative symmetric encryption scheme

\[ \{\{m\}\}_{k_1} \}_{k_2} = \{\{m\}\}_{k_2} \}_{k_1} \]

where \( \{m\}_k \) denotes the encryption of message \( m \) under the key \( k \)

Example: RSA

No authentication!

since \( \{\{\text{pin: 3443}\}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}\}_{pk_B}\}_{pk_A} \) by commutativity
Example of a logical attack

Assume a commutative symmetric encryption scheme

\[
\{\{m\}_k\}_k = \{\{m\}_k\}_k
\]

where \(\{m\}_k\) denotes the encryption of message \(m\) under the key \(k\)

Example: RSA

No authentication!

since \(\{\{\text{pin: 3443}\}_k\}_k\) by commutativity
Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[ A \]

\[ B \]

\[ \text{new} N_A \]

\[ \text{new} N_B \]

\[ \text{aenc}(pk_A, \langle N_A, N_B \rangle) \]

\[ \text{aenc}(pk_B, \langle N_B, A \rangle) \]

\[ k_{AB} \leftarrow h(N_A, N_B) \]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[ \text{new } N_A \]

\[ A \]

\[ B \]

\[ k_{AB} \leftarrow h(N_A, N_B) \]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[ A \rightarrow B \text{ aenc}(pk_B, \langle N_A, A \rangle) \rightarrow \text{ aenc}(pk_A, \langle N_B, A \rangle) \rightarrow k_{AB} \leftarrow h(N_A, N_B) \]

**Needham-Schroeder Public Key (NSPK)**

NSPK: authentication and key agreement protocol

\[
A \quad \xrightarrow{\text{new } N_A} \quad B
\]

\[
aenc(pk_B, \langle N_A, A \rangle) \xrightarrow{\text{new } N_B} \text{key } k_{AB} \leftarrow h(N_A, N_B)
\]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[
A \quad \xrightarrow{\text{new } N_A} \quad B \quad \xleftarrow{\text{new } N_B}
\]

\[
\text{aenc}(\text{pk}_B, \langle N_A, A \rangle) \quad \rightarrow \quad \text{aenc}(\text{pk}_A, \langle N_A, N_B \rangle)
\]

**Needham-Schroeder Public Key (NSPK)**

NSPK: authentication and key agreement protocol

\[\text{new } N_A\rightarrow A \rightarrow B \rightarrow \text{new } N_B\]

\[\text{aenc}(pk_B, \langle N_A, A \rangle)\]

\[\text{aenc}(pk_A, \langle N_A, N_B \rangle)\]

\[\text{aenc}(pk_B, \langle N_B, A \rangle)\]

\[k_{AB} \leftarrow h(N_A, N_B)\]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[ k_{AB} \leftarrow h(N_A, N_B) \]

NSPK: security requirements

- **Authentication:** if Alice has completed the protocol, apparently with Bob, then Bob must also have completed the protocol with Alice.

- **Authentication:** If Bob has completed the protocol, apparently with Alice, then Alice must have completed the protocol with Bob.

- **Confidentiality:** Messages sent encrypted with the agreed key $(k \leftarrow h(N_A, N_B))$ remain secret.
NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!
NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ A \]
\[ \text{new } N_A \]

\[ I \]

\[ B \]

\[ k_{AI} \leftarrow h(N_A, N_B) \]

\[ k_{AB} \leftarrow h(N_A, N_B) \]

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[
\text{\textbf{A}} \quad \text{new} \quad N_A \quad \xrightarrow{\text{aenc(pk}_I,\langle N_A, A \rangle)} \quad \text{I} \\
\text{\textbf{B}} \quad \xrightarrow{\text{aenc(pk}_I,\langle N_A, A \rangle)} \quad \text{new} \quad N_B \\
\text{\textbf{A}} \quad \xrightarrow{\text{aenc(pk}_I,\langle N_A, N_B \rangle)} \quad \text{I} \\
\text{\textbf{B}} \quad \xrightarrow{\text{aenc(pk}_I,\langle N_A, N_B \rangle)} \quad \text{new} \quad N_B
\]

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[
\begin{align*}
A & \quad I \quad B \\
\text{new } N_A & \quad \text{aenc}(pk_I, \langle N_A, A \rangle) & \quad \text{aenc}(pk_B, \langle N_A, A \rangle) \\
\end{align*}
\]

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ A \]

\[ \text{new } N_A \]

\[ \text{aenc}(pk_I, \langle N_A, A \rangle) \]

\[ I \]

\[ \text{aenc}(pk_B, \langle N_A, A \rangle) \]

\[ B \]

\[ \text{new } N_B \]

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ A \]
new \( N_A \)

\[ I \]
aenc(\( pk_A \),\( \langle N_A, A \rangle \))

\[ B \]
new \( N_B \)
aenc(\( pk_B \),\( \langle N_A, A \rangle \))
aenc(\( pk_A \),\( \langle N_A, N_B \rangle \))

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[
\begin{align*}
A \quad & \quad \text{new } N_A \\
& \quad \downarrow \quad \text{aenc}(pk_i, \langle N_A, A \rangle) \\
& \quad \downarrow \quad \text{aenc}(pk_A, \langle N_A, N_B \rangle) \\
I \quad & \quad \uparrow \quad \text{aenc}(pk_B, \langle N_A, A \rangle) \\
& \quad \uparrow \quad \text{aenc}(pk_A, \langle N_A, N_B \rangle) \\
B \quad & \quad \text{new } N_B
\end{align*}
\]

NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ \text{[G. Lowe. “An attack on the Needham-Schroeder public key authentication protocol”. Information Processing Letters (November 1995)]} \]
NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ G. \text{ Lowe. “An attack on the Needham-Schroeder public key authentication protocol”. Information Processing Letters (November 1995).} \]
NSPK: Lowe’s attack on authentication

Attack found 17 years after the publication of the NS protocol!!

\[ A \]

new \( N_A \)

\[
aenc(pk_I, \langle N_A, A \rangle) \]

\[
aenc(pk_A, \langle N_A, N_B \rangle) \]

\[
aenc(pk_I, \langle N_B, A \rangle) \]

\[
k_{AI} \leftarrow h(N_A, N_B) \]

\[
k_{AB} \leftarrow h(N_A, N_B) \]

\[ I \]

\[
k_{AI} \leftarrow h(N_A, N_B) \]

\[
k_{AB} \leftarrow h(N_A, N_B) \]

\[ B \]

new \( N_B \)

\[
aenc(pk_B, \langle N_A, A \rangle) \]

\[
aenc(pk_A, \langle N_A, N_B \rangle) \]

\[
aenc(pk_B, \langle N_B, A \rangle) \]

**NSPK: Lowe’s fix**

\[ k_{AB} \leftarrow h(N_A, N_B) \]

Diagram:

- **A**
  - new \( N_A \)
  - \( aenc(pk_B, \langle N_A, A \rangle) \)
  - \( aenc(pk_A, \langle N_A, \langle N_B, B \rangle \rangle) \)
  - \( k_{AB} \leftarrow h(N_A, N_B) \)

- **B**
  - new \( N_B \)
  - \( aenc(pk_B, \langle N_B, A \rangle) \)
  - \( aenc(pk_A, \langle N_A, \langle N_B, B \rangle \rangle) \)
  - \( k_{AB} \leftarrow h(N_A, N_B) \)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

- \{m\}^s_k: message \(m\) symmetrically encrypted under key \(k\)
- \{m\}^a_k: message \(m\) asymmetrically encrypted under key \(k\)
- \([m]_k\): message \(m\) digitally signed with key \(k\)
- \(t_C, t_K\): timestamps
- \(TGT = \{AK, C, t_K\}^s_{k_T}\)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

\[ C \quad \text{KAS} \]

- \( \{m\}_k^s \): message \( m \) symmetrically encrypted under key \( k \)
- \( \{m\}_k^a \): message \( m \) asymmetrically encrypted under key \( k \)
- \( [m]_k \): message \( m \) digitally signed with key \( k \)
- \( t_C, t_K \): timestamps
- \( TGT = \{AK, C, t_K\}_k^s \)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

\[ C \quad \text{new } n_1, n_2 \quad \text{KAS} \]

- \( \{m\}^s_k \): message \( m \) symmetrically encrypted under key \( k \)
- \( \{m\}^a_k \): message \( m \) asymmetrically encrypted under key \( k \)
- \([m]_k \): message \( m \) digitally signed with key \( k \)
- \( t_C, t_K \): timestamps
- \( TGT = \{AK, C, t_K\}^s_{k_T} \)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

\[
\begin{align*}
C & \quad \text{new } n_1, n_2 \\
\text{Cert}_C, [t_C, n_2]_{s_k_C}, C, T, n_1 & \quad \rightarrow \\
\text{KAS} & \\
\end{align*}
\]

- \{m\}_k^s: message \( m \) symmetrically encrypted under key \( k \)
- \{m\}_k^a: message \( m \) asymmetrically encrypted under key \( k \)
- \[m\]_k: message \( m \) digitally signed with key \( k \)
- \( t_C, t_K \): timestamps
- \( TGT = \{AK, C, t_K\}_k^s \)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

\[ C \xrightarrow{\text{new } n_1, n_2} \text{Cert}_C, [t_C, n_2]_{sk_C}, C, T, n_1 \xrightarrow{\text{new } k, AK} KAS \]

- \( \{m\}_k^s \): message \( m \) symmetrically encrypted under key \( k \)
- \( \{m\}_k^a \): message \( m \) asymmetrically encrypted under key \( k \)
- \( [m]_k \): message \( m \) digitally signed with key \( k \)
- \( t_C, t_K \): timestamps
- \( TGT = \{AK, C, t_K\}_k^s \)
Public Key Kerberos PKINIT-26 (very abstract)

Goals: client authentication, key agreement, TGT delivery

\[\begin{align*}
C & \quad \text{new } n_1, n_2 \\
\text{Cert}_C, [t_C, n_2]_{sk_C}, C, T, n_1 & \quad \text{\rightarrow} \\
\{\text{Cert}_K, [k, n_2]_{sk_K}\}^{a}_{pk_C}, C, \text{TGT}, \{\text{AK}, n_1, t_K, T\}^{s}_k & \quad \text{\leftarrow}
\end{align*}\]

- \(\{m\}^{s}_k\): message \(m\) symmetrically encrypted under key \(k\)
- \(\{m\}^{a}_k\): message \(m\) asymmetrically encrypted under key \(k\)
- \([m]_k\): message \(m\) digitally signed with key \(k\)
- \(t_C, t_K\): timestamps
- \(\text{TGT} = \{\text{AK}, C, t_K\}^{s}_{k_T}\)
PKINIT-26: attack

PKINIT-26: attack

\[
\begin{array}{c}
C \\
\text{new } n_1, \ n_2 \\
\end{array}
\quad
\begin{array}{c}
I \\
\end{array}
\quad
\begin{array}{c}
KAS \\
\end{array}
\]

PKINIT-26: attack

PKINIT-26: attack

\[\text{new } n_1, n_2\]

\[\text{Cert}_C, [t_{C,n_2}]_{sk_C}, C, T, n_1\rightarrow\text{I}\]

\[\text{Cert}_I, [t_{C,n_2}]_{sk_I}, I, T, n_1\rightarrow\text{new } k, AK\]

PKINIT-26: attack

\[Cert_C, [t_C, n_2]_{sk_C}, C, T, n_1 \rightarrow \]

\[Cert_I, [t_C, n_2]_{sk_I}, I, T, n_1 \rightarrow \]

new \(k, AK\)

\[\{Cert_K, [k, n_2]_{sk_K}\}^{a}_{pk_I} \leftarrow l, TGT, \{AK, n_1, t_K, T\}^{s}_k\]