Cryptographic protocols

Myrto Arapinis
School of Informatics
University of Edinburgh

October 20, 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
The attacker controls the network (1)
The attacker controls the network (2)

Verizon, BT, Vodafone, Level 3 'let NSA jack into Google, Yahoo! fiber'

Telcos cooperated with g-men in data slurp, claim sources

27 Nov 2013 at 02:19, Shaun Nichols

In October, NSA whistleblower Edward Snowden claimed Uncle Sam's spies tapped into the optic-fiber
The attacker controls the network (3)
All messages can be intercepted by an attacker (1)
All messages can be intercepted by an attacker (2)
An attacker can intercept packets, but also alter, forge new, and inject packets.
More complex systems needed...
More complex systems needed...

\[
ext = E(K_E, \text{Transfer 100 € on Amazon’s account}) \quad m = MAC(K_M, E(K_E, \text{Transfer 100 € on Amazon’s account}))
\]
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
... to achieve more complex properties

- **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”
And end up in the news :(

**FREAK: Another day, another serious SSL security hole**

More than one third of encrypted Websites are open to attack via the FREAK security hole.

**The Telegraph**

**Defects in e-passports allow real-time tracking**

This threat brought to you by RFID

**threatpost**

**TRIPLE HANDSHAKE ATTACKS TARGET TLS RESUMPTION, RENEGOTIATION**
Many of these attacks do not even break the crypto primitives!!
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
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

\[
\left\{ \left\{ m \right\} k_1 \right\} k_2 = \left\{ \left\{ m \right\} k_2 \right\} k_1
\]

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

$$\begin{array}{c|c}
A & B \\
\{\text{pin: 3443}\}_{pk_A} & \{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} \\
\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} & \{\text{pin: 3443}\}_{pk_B} \\
\{\text{pin: 3443}\}_{pk_B} & \{\text{pin: 3443}\}_{pk_B}\end{array}$$

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

\[
\text{\{\{m\}\}_k}_1 \cdot \text{\{\{m\}\}_k}_2 = \text{\{\{m\}\}_k}_2 \cdot \text{\{\{m\}\}_k}_1
\]

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

Example: RSA

No authentication!

since \(\text{\{\{\text{pin: 3443}\}_p}{k_A}\}_p{k_B} = \text{\{\{\text{pin: 3443}\}_p}{k_B}\}_p{k_A}\) 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!

\[\begin{array}{c}
A \\
\{\text{pin: 3443}\}_{pk_A} \\
\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} \\
\{\text{pin: 3443}\}_{pk_B} \\
B \\
A \\
I
\end{array}\]

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

Assume a commutative symmetric encryption scheme

\[ \{ \{ m \} _k \} _k \cdot k_2 = \{ \{ m \} _k \} _k \cdot k_1 \]

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
Authentication and key agreement protocols
Authentication and key agreement

- Long-term keys should be used as little as possible to reduce “attack-surface”

- The use of a key should be restricted to a specific purpose e.g. you shouldn’t use the same RSA key both for encryption and signing

- Public key algorithms tend to be computationally more expensive than symmetric key algorithms

--> Long-term keys are used to establish short-term session keys e.g. TLS over HTTP, AKA for 3G, BAC for epassports, etc.
Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[ A \] \[ B \]

\[ A \rightarrow A^\text{enc}(pk_B, \langle N_A, A \rangle) \]

\[ \leftarrow B^\text{enc}(pk_A, \langle N_A, N_B \rangle) \]

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

NSPK: authentication and key agreement protocol

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

\[ a\text{enc}(pk_B, \langle N_A, A \rangle) \rightarrow a\text{enc}(pk_A, \langle N_A, N_B \rangle) \]

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

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

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

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[
\begin{align*}
A & \xrightarrow{\text{new } N_A} \quad \text{aenc}(\text{pk}_B, \langle N_A, A \rangle) \quad \xrightarrow{\text{new } N_B} B \\
\quad \text{aenc}(\text{pk}_B, \langle N_A, A \rangle) \quad \xrightarrow{\text{h}(N_A, N_B)} \quad k_{AB}
\end{align*}
\]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

A

new $N_A$

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

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

new $N_B$

B

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

A

\[
\text{new } N_A
\]

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

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

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

B

\[
\text{new } N_B
\]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

\[
\begin{align*}
A & \quad \text{new } N_A \\
& \quad \text{aenc}(\text{pk}_B, \langle N_A, A \rangle) \\
& \quad \text{aenc}(\text{pk}_A, \langle N_A, N_B \rangle) \\
& \quad \text{aenc}(\text{pk}_B, \langle N_B, A \rangle) \\
& \quad k_{AB} \leftarrow h(N_A, N_B)
\end{align*}
\]

\[
\begin{align*}
& \quad \text{new } N_B \\
& \quad \text{aenc}(\text{pk}_A, \langle N_A, N_B \rangle) \\
& \quad \text{aenc}(\text{pk}_B, \langle N_B, A \rangle) \\
& \quad k_{AB} \leftarrow h(N_A, N_B)
\end{align*}
\]

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 \( k \leftarrow h(N_A, NB) \) 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!!

\[
\text{new } N_A \quad I \quad B
\]

NSPK: Lowe’s attack on authentication

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

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

NSPK: Lowe’s attack on authentication

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

\[
\text{A} \quad \text{I} \quad \text{B}
\]

\[
\text{new } N_A \quad \text{aenc}(pk_I, \langle N_A, A \rangle) \quad \text{aenc}(pk_B, \langle N_A, A \rangle) \quad k_{AI} \leftarrow h(N_A, N_B) \quad k_{IB} \leftarrow h(N_A, N_B) \quad k_{AB} \leftarrow h(N_A, N_B)
\]

NSPK: Lowe’s attack on authentication

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

NSPK: Lowe’s attack on authentication

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

\[ A \]

new \( N_A \)

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

\[ I \]

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

\[ B \]

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

NSPK: Lowe’s attack on authentication

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

\[ A \]
- new \( N_A \)
  \( A \rightarrow I \):
  \[ \text{aenc}(\text{pk}_I, \langle N_A, A \rangle) \]
  \( I \rightarrow B \):
  \[ \text{aenc}(\text{pk}_B, \langle N_A, A \rangle) \]
  \( B \rightarrow A \):
  \[ \text{aenc}(\text{pk}_A, \langle N_A, N_B \rangle) \]

\[ B \]
- new \( N_B \)
  \( B \rightarrow A \):
  \[ \text{aenc}(\text{pk}_A, \langle N_A, N_B \rangle) \]
  \( A \rightarrow I \):
  \[ \text{aenc}(\text{pk}_I, \langle N_A, A \rangle) \]

NSPK: Lowe’s attack on authentication

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

\[ A \]
- new \( N_A \)
  - \( aenc(pk_I, \langle N_A, A \rangle) \)
  - \( aenc(pk_A, \langle N_A, N_B \rangle) \)
  - \( aenc(pk_I, \langle N_B, A \rangle) \)

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

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

NSPK: Lowe’s attack on authentication

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

\[ A \]

\[ \text{new } N_A \]

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

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

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

\[ B \]

\[ \text{new } N_B \]

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

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

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

NSPK: Lowe’s attack on authentication

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

\[ A \]

\[ \text{new } N_A \]

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

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

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

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

\[ I \]

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

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

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

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

\[ B \]

\[ \text{new } N_B \]

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

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

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

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

NSPK: Lowe’s fix

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

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

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

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

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