Cryptographic protocols

Myrto Arapinis
School of Informatics
University of Edinburgh

October 20, 2016

Context

Applications exchanging sensitive data over a public network:

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

Context

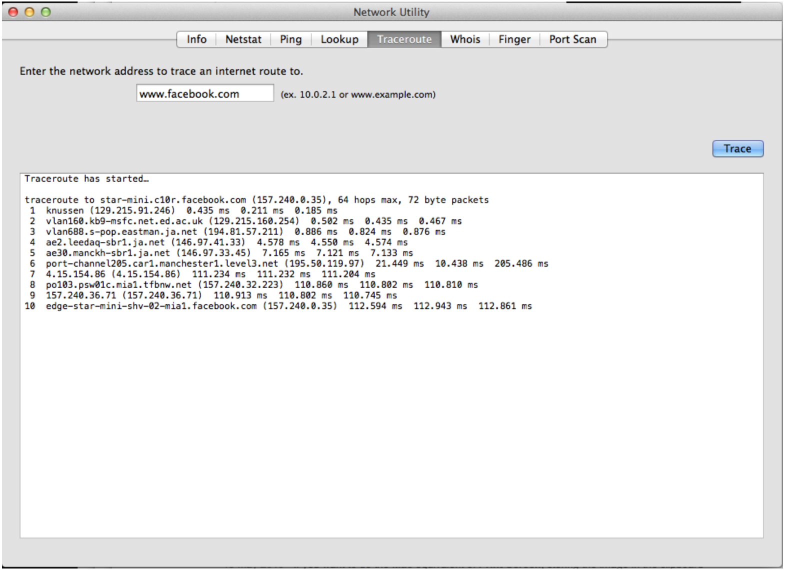
Applications exchanging sensitive data over a public network:

- 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
  $\longrightarrow$ the network is the attacker
- control dishonest participants

The attacker controls the network (1)



The attacker controls the network (2)

The Register®

Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE

Networks

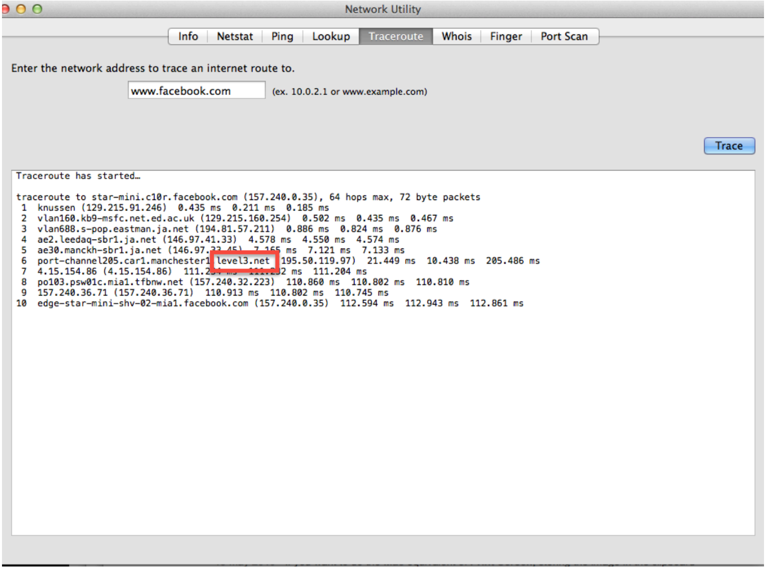
Verizon, BT, Vodafone, Level 3 'let NSA jack into Google, Yahoo! fiber'

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

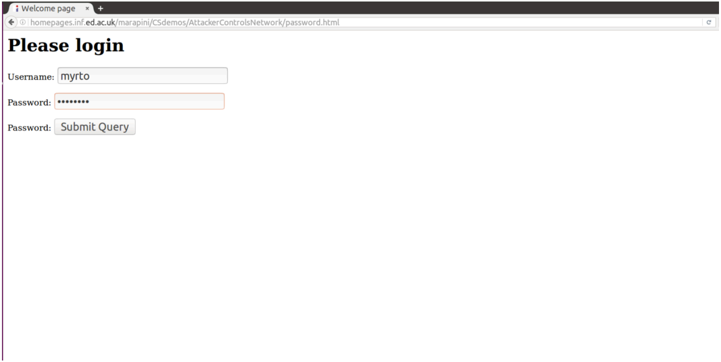
27 Nov 2013 at 02:19, Shaun Nicholas 2

In October, NSA whistleblower Edward Snowden claimed Uncle Sam's spies tapped into the optic-fiber

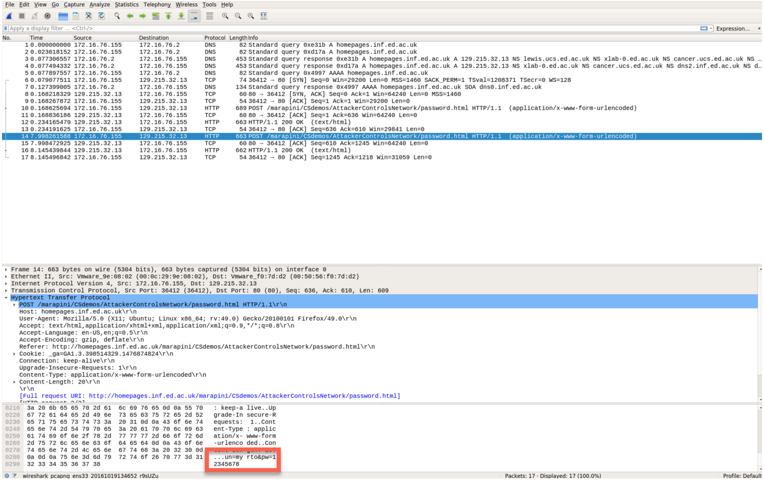
The attacker controls the network (3)



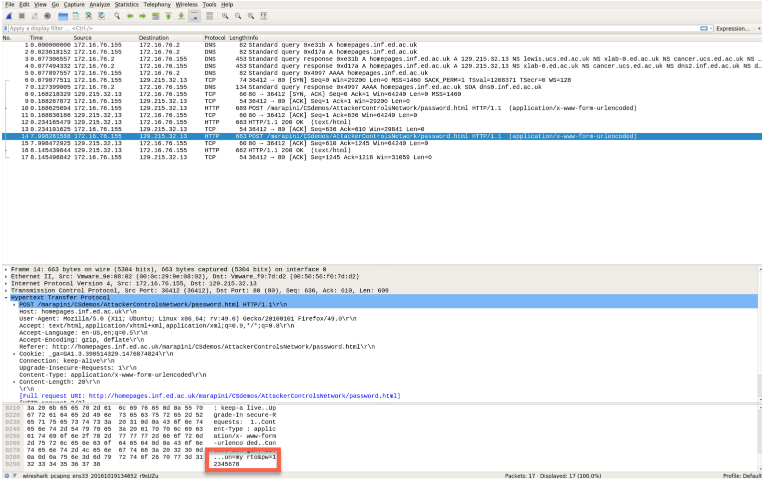
All messages can be intercepted by an attacker (1)



All messages can be intercepted by an attacker (2)



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...

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

BNP PARIBAS

More complex systems needed...

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

BNP PARIBAS

Replay attack

$\xrightarrow{(e,m)}$

$\xrightarrow{(e,m)}$

$\vdots$

$\xrightarrow{(e,m)}$

BNP PARIBAS

... 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 an 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

Cryptographic protocols

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

Cryptographic protocols

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"

Single-Sign-On protocol - A. Armando, R. Carbone, L. Compagna, J. Cuellar, and M. L. Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps"

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 :(

EDITION: UK

ZDNet

MICROSOFT STORAGE INNOVATION HARDWARE APPLE MORE NEWSLETTERS ALL WRITERS

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

Home Video News World Sport Business Money Comment Culture Travel Life W

USA | Asia | China | Europe | Middle East | Australasia | Africa | South America | Central Asia

HOME » NEWS » WORLD NEWS » NORTH AMERICA » USA

Hacker remotely crashes Jeep from 10 miles away

Security experts warn that more than 470,000 cars made by Fiat Chrysler could be at risk of being attacked by similar means – including those driven in the UK

The Register®

Biting the hand that feeds IT

Defects in e-passports allow real-time tracking

This threat brought to you by RFID

threatpost

CATEGORIES FEATURED PODCASTS VIDEOS

TRIPLE HANDSHAKE ATTACKS TARGET TLS RESUMPTION, RENEGOTIATION

Logical attacks

Many of these attacks do not even break the crypto primitives!!

Example of a logical attack

Assume a commutative symmetric encryption scheme

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

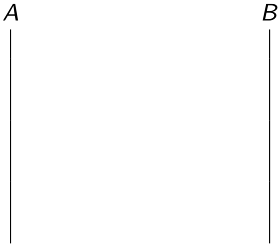
where $\{m\}_k$ denotes the encryption of message m under the key k
Example: RSA

Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\{\{m\}_{\color{red}k_1}\}_{\color{red}k_2} = \{\{m\}_{\color{red}k_2}\}_{\color{red}k_1}$$

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

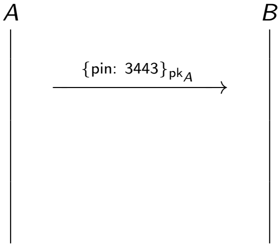


Example of a logical attack

Assume a commutative symmetric encryption scheme

$$\{\{m\}_{\color{red}k_1}\}_{\color{red}k_2} = \{\{m\}_{\color{red}k_2}\}_{\color{red}k_1}$$

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

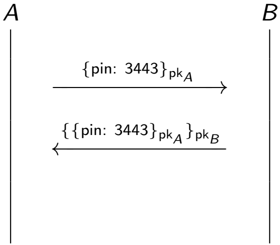


Example of a logical attack

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

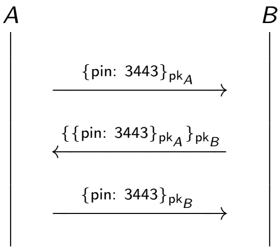


Example of a logical attack

Assume a commutative symmetric encryption scheme

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

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



since $\{\{\text{pin: } 3443\}_{\text{pk}_A}\}_{\text{pk}_B} = \{\{\text{pin: } 3443\}_{\text{pk}_B}\}_{\text{pk}_A}$ by commutativity

Example of a logical attack

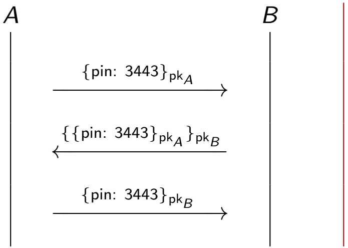
Assume a commutative symmetric encryption scheme

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

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

Example: RSA

No authentication!



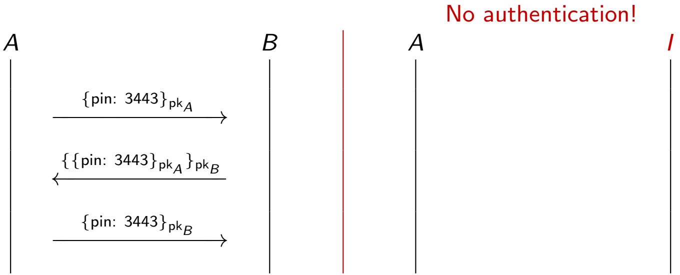
since $\{\{\text{pin: } 3443\}_{\text{pk}_A}\}_{\text{pk}_B} = \{\{\text{pin: } 3443\}_{\text{pk}_B}\}_{\text{pk}_A}$ by commutativity

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



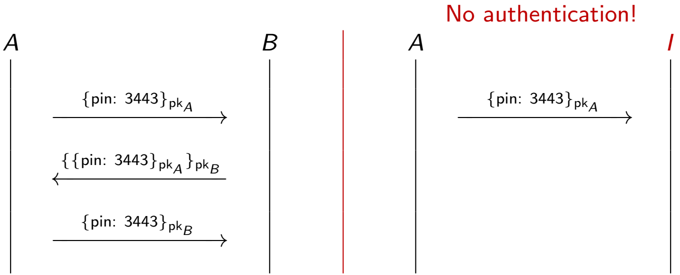
since $\{\{\text{pin: } 3443\}_{\mathrm{pk}_A}\}_{\mathrm{pk}_B} = \{\{\text{pin: } 3443\}_{\mathrm{pk}_B}\}_{\mathrm{pk}_A}$ by commutativity

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



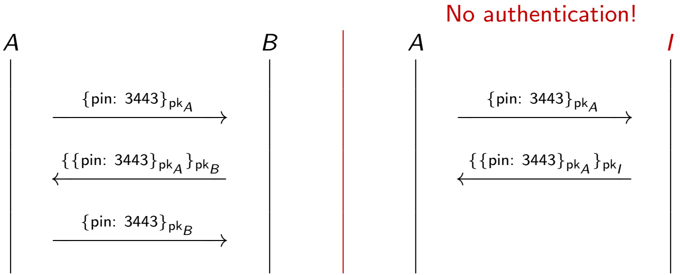
since $\{\{\text{pin: } 3443\}_{\text{pk}_A}\}_{\text{pk}_B} = \{\{\text{pin: } 3443\}_{\text{pk}_B}\}_{\text{pk}_A}$ by commutativity

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



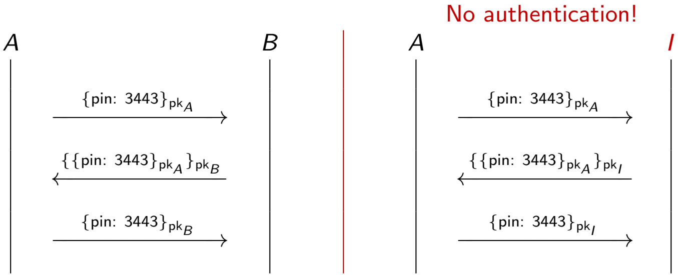
since $\{\{\text{pin: } 3443\}_{\mathsf{pk}_A}\}_{\mathsf{pk}_B} = \{\{\text{pin: } 3443\}_{\mathsf{pk}_B}\}_{\mathsf{pk}_A}$ by commutativity

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



since $\{\{\text{pin: } 3443\}_{\text{pk}_A}\}_{\text{pk}_B} = \{\{\text{pin: } 3443\}_{\text{pk}_B}\}_{\text{pk}_A}$ by commutativity

Authentication and key agreement protocols

Authentication and key agreement

- Long-term keys should be used as little as possible to to reduce "attack-srufarce"
- 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

$\rightsquigarrow$ 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

[N. Roger, M. Schroeder, Michael. “Using encryption for authentication in large networks of computers”. Communications of the ACM (December 1978)]

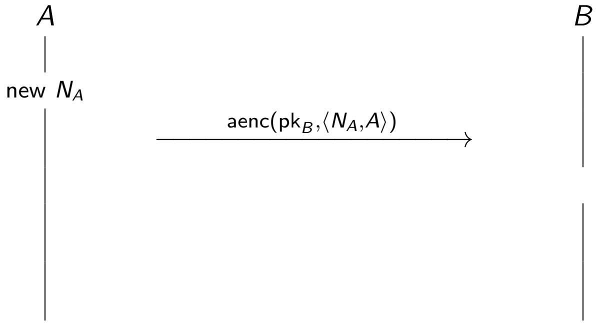
Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

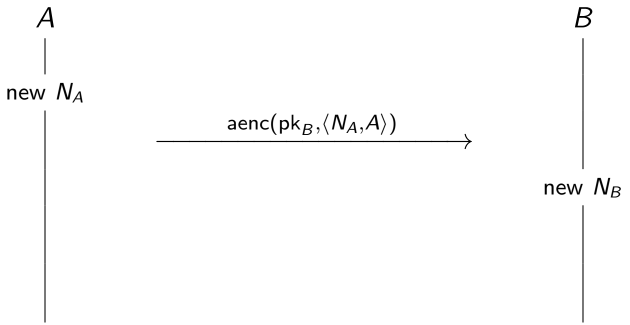
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

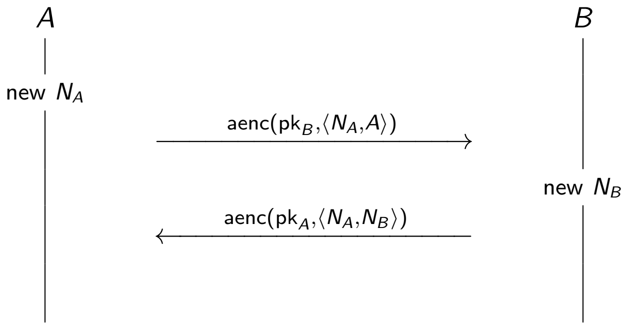
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

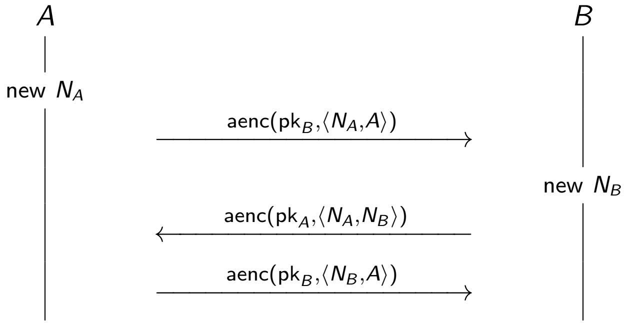
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

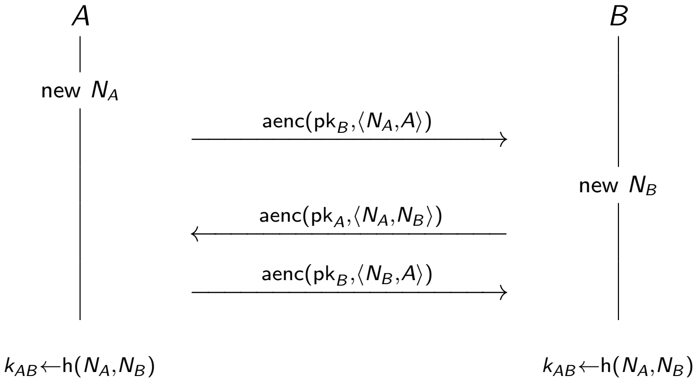
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. “Using encryption for authentication in large networks of computers”. Communications of the ACM (December 1978)]

NSPK: security requirements

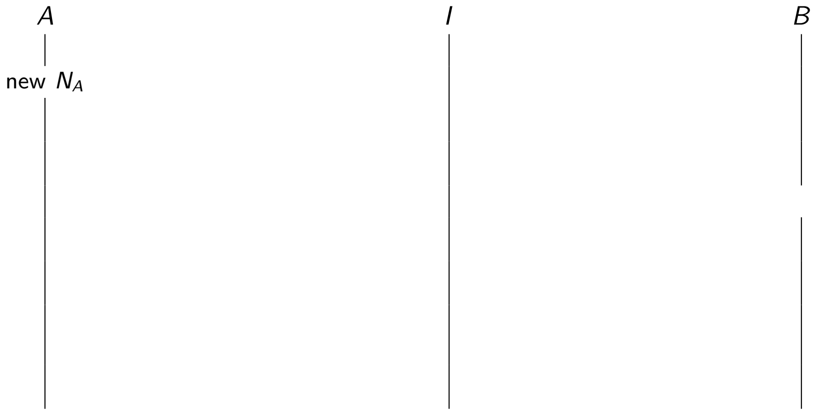
- Authentication: if Alice has completed the protocol, apparently with Bob, then Bob must also have completed the protocol with Alice.
- Authentication: If Bob has completed the protocol, apparently with Alice, then Alice must have completed the protocol with Bob.
- Confidentiality: Messages sent encrypted with the agreed key ($k \leftarrow \mathrm{h}(N_A, NB)$) 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

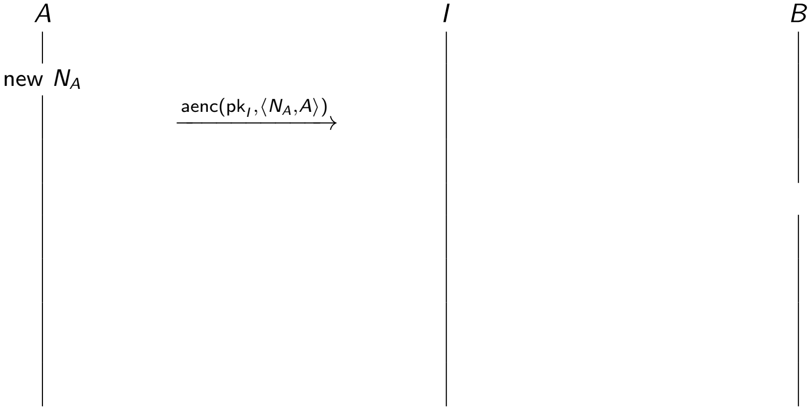
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

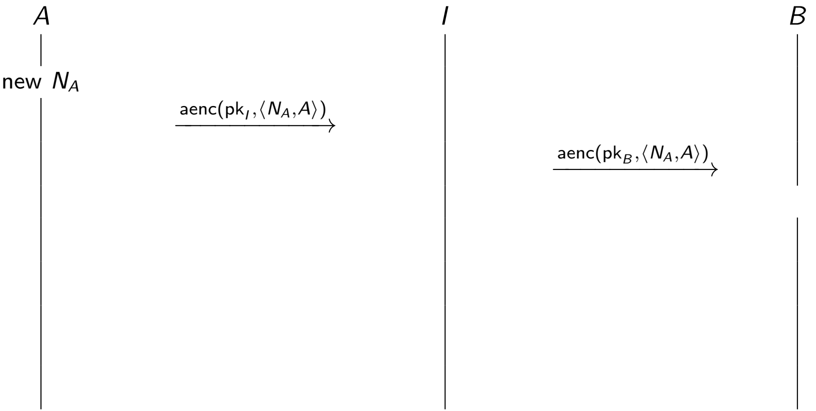
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

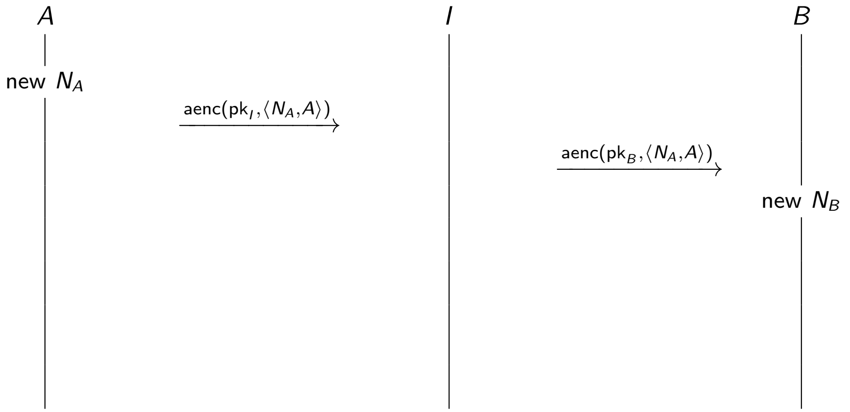
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

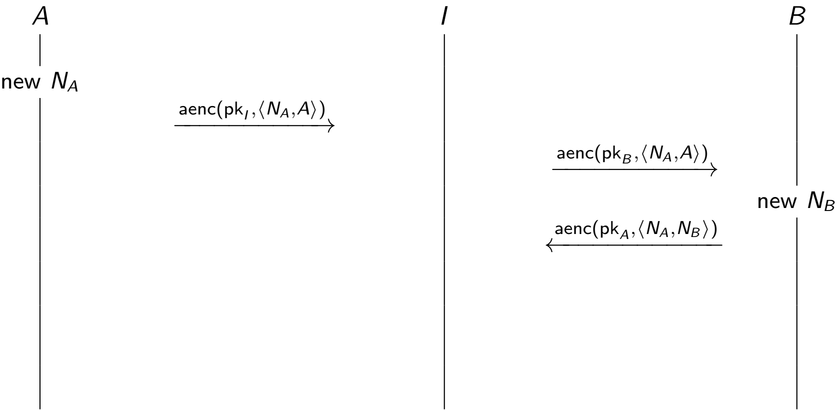
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

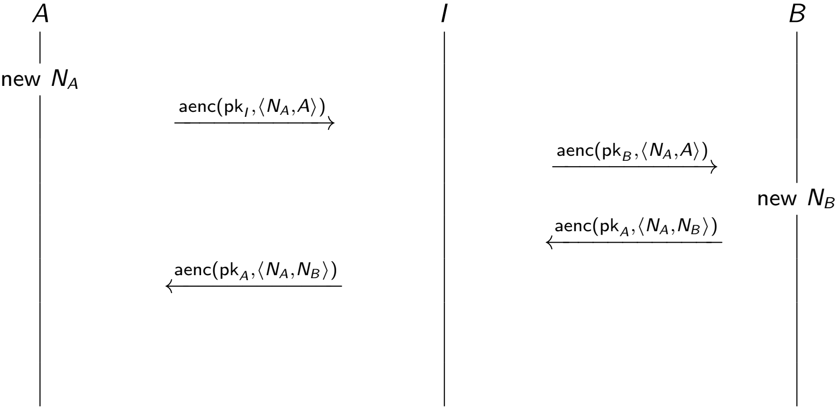
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

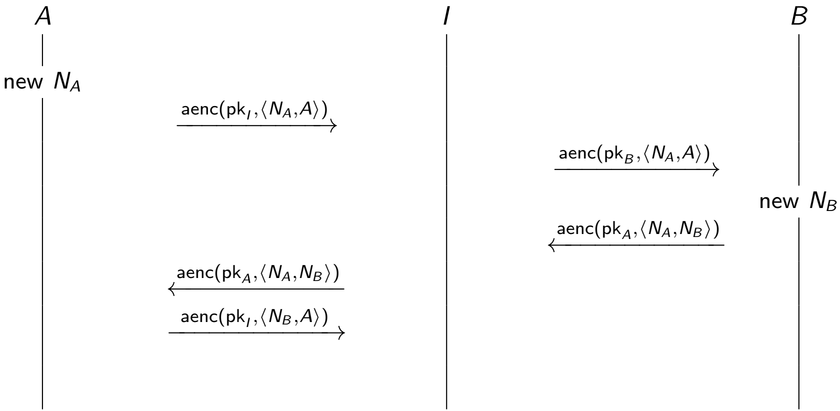
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

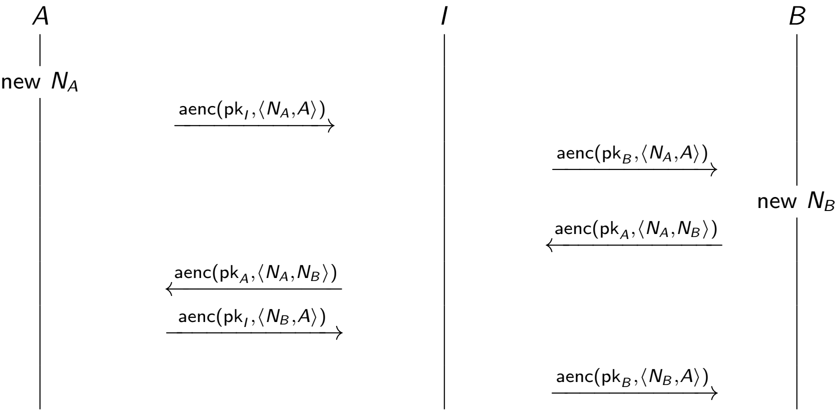
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

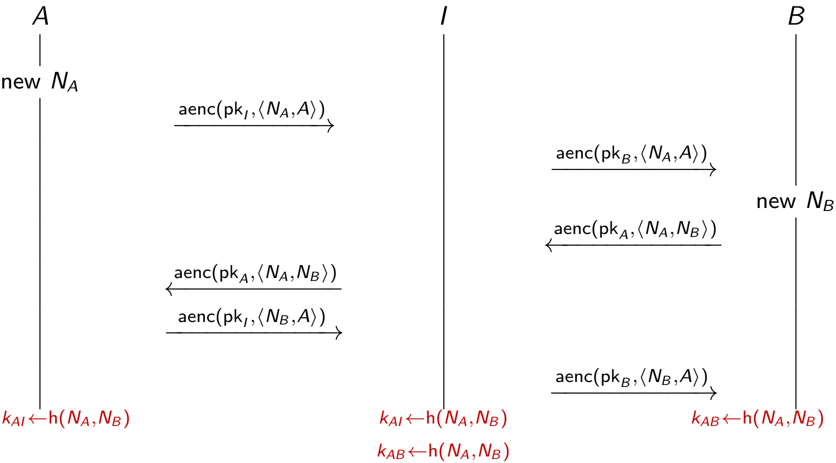
Attack found 17 years after the publication of the NS protocol!!



[G. 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. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's fix