

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

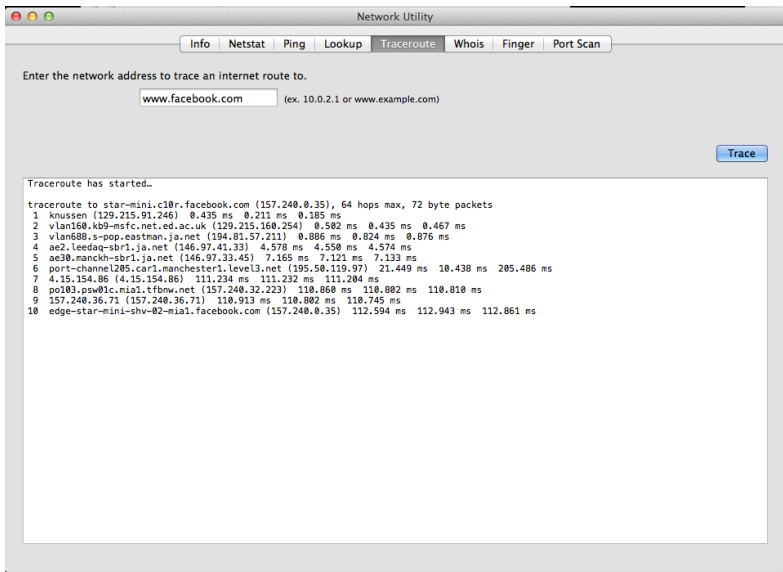
Applications exchanging **sensitive data** over a **public network**:

- ▶ 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
→ **the network is the attacker**
- ▶ control dishonest participants

The attacker controls the network (1)



The attacker controls the network (2)

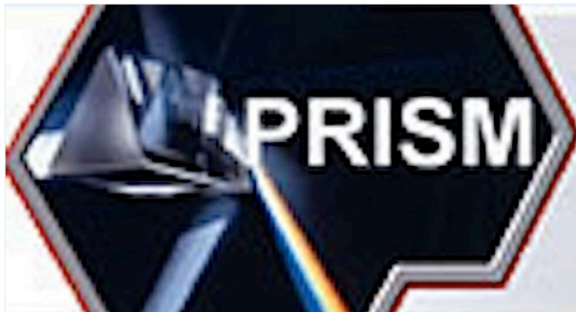


[DATA CENTRE](#) [SOFTWARE](#) [NETWORKS](#) [SECURITY](#) [TRANSFORMATION](#) [DEVOPS](#) [BUSINESS](#) [HARDWARE](#)

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 Nichols](#)



2



In October, NSA whistleblower Edward Snowden claimed Uncle Sam's spies [tapped into the optic-fiber](#)

4 / 19

The attacker controls the network (3)

The screenshot shows a 'Network Utility' window with the 'Traceroute' tab selected. The input field contains 'www.facebook.com'. The 'Trace' button is visible. The output shows the traceroute path to star-mini.c10r.facebook.com (157.240.0.35), 64 hops max, 72 byte packets. The path includes several hops, with 'level3.net' highlighted in a red box at hop 6.

Traceroute has started.

traceroute to star-mini.c10r.facebook.com (157.240.0.35), 64 hops max, 72 byte packets

| Hop | IP Address | RTT 1 | RTT 2 | RTT 3 | RTT 4 |
|-----|---|------------|------------|------------|-------|
| 1 | knussen (129.215.91.246) | 0.435 ms | 0.211 ms | 0.185 ms | |
| 2 | vlan160.kb9-msfc.net.ed.ac.uk (129.215.160.254) | 0.502 ms | 0.435 ms | 0.467 ms | |
| 3 | vlan688.s-pop.eastman.ja.net (194.81.57.211) | 0.886 ms | 0.824 ms | 0.876 ms | |
| 4 | ae2.leedaq-sbr1.ja.net (146.97.41.33) | 4.578 ms | 4.550 ms | 4.574 ms | |
| 5 | ae30.manckh-sbr1.ja.net (146.97.22.45) | 7.165 ms | 7.121 ms | 7.133 ms | |
| 6 | port-channel205.car1.manchester1.level3.net (195.50.119.97) | 21.449 ms | 10.438 ms | 205.486 ms | |
| 7 | 4.15.154.86 (4.15.154.86) | 111.249 ms | 111.284 ms | | |
| 8 | po103.psv01c.mia1.tfbnw.net (157.240.32.223) | 110.860 ms | 110.802 ms | 110.810 ms | |
| 9 | 157.240.36.71 (157.240.36.71) | 110.913 ms | 110.802 ms | 110.745 ms | |
| 10 | edge-star-mini-shv-02-mia1.facebook.com (157.240.0.35) | 112.594 ms | 112.943 ms | 112.861 ms | |

All messages can be intercepted by an attacker (1)

Welcome page

homepages.inf.ed.ac.uk/marapini/C5demos/AttackerControlsNetwork/password.html

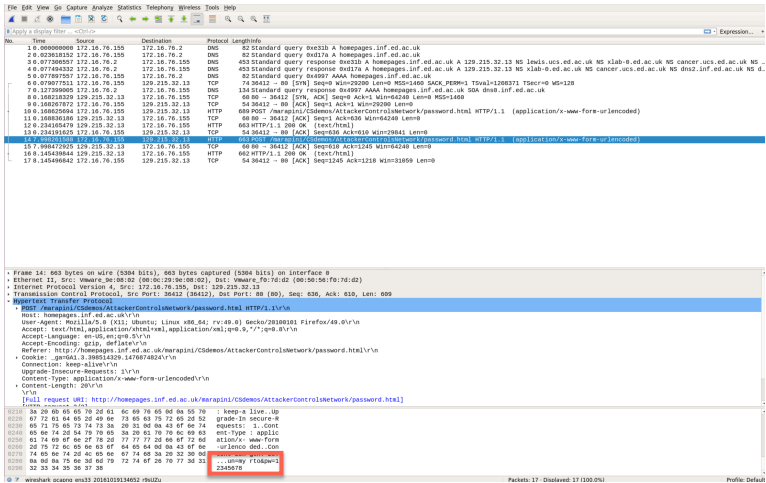
Please login

Username:

Password:

Password:

All messages can be intercepted by an attacker (2)



All messages can be intercepted by an attacker (2)

The image shows a Wireshark packet capture of network traffic. The top pane displays a list of packets, with packet 14 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request for a password form. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|--|
| 1 | 0.000000000 | 172.16.76.155 | 172.16.76.2 | DNS | 82 | Standard query 0x3317 A homepages.inf.ed.ac.uk |
| 2 | 0.023613152 | 172.16.76.155 | 172.16.76.2 | DNS | 82 | Standard query 0x3317 A homepages.inf.ed.ac.uk |
| 3 | 0.077306597 | 172.16.76.2 | 172.16.76.155 | DNS | 453 | Standard query response 0x3317 A homepages.inf.ed.ac.uk A 129.215.32.13 NS lewis.ucs.ed.ac.uk NS cancer.ucs.ed.ac.uk NS d... |
| 4 | 0.077494332 | 172.16.76.2 | 172.16.76.155 | DNS | 453 | Standard query response 0x3317 A homepages.inf.ed.ac.uk A 129.215.32.13 NS lewis.ucs.ed.ac.uk NS cancer.ucs.ed.ac.uk NS d... |
| 5 | 0.077607507 | 172.16.76.155 | 172.16.76.2 | DNS | 82 | Standard query 0x4997 AAAA homepages.inf.ed.ac.uk |
| 6 | 0.079077531 | 172.16.76.155 | 129.215.32.13 | TCP | 74 | 345612 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1208371 TSecr=0 WS=128 |
| 7 | 0.127339000 | 172.16.76.2 | 172.16.76.155 | DNS | 134 | Standard query response 0x4997 AAAA homepages.inf.ed.ac.uk SDA dmba.inf.ed.ac.uk |
| 8 | 0.160218329 | 129.215.32.13 | 172.16.76.155 | TCP | 60 | 80 → 345612 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 9 | 0.160287872 | 172.16.76.155 | 129.215.32.13 | TCP | 54 | 345612 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0 |
| 10 | 0.160625694 | 172.16.76.155 | 129.215.32.13 | HTTP | 608 | POST /marapini/CSdemos/AttackerControlNetwork/password.html HTTP/1.1 (application/x-www-form-urlencoded) |
| 11 | 0.160836186 | 129.215.32.13 | 172.16.76.155 | TCP | 60 | 80 → 345612 [ACK] Seq=1 Ack=636 Win=64240 Len=0 |
| 12 | 0.234165471 | 129.215.32.13 | 172.16.76.155 | HTTP | 663 | HTTP/1.1 200 OK [text/html] |
| 13 | 0.234191629 | 129.215.32.13 | 129.215.32.13 | TCP | 54 | 345612 → 80 [ACK] Seq=636 Ack=610 Win=29841 Len=0 |
| 14 | 0.234211171 | 172.16.76.155 | 129.215.32.13 | HTTP | 663 | GET /marapini/CSdemos/AttackerControlNetwork/password.html HTTP/1.1 (application/x-www-form-urlencoded) |
| 15 | 1.090472923 | 129.215.32.13 | 172.16.76.155 | TCP | 60 | 80 → 345612 [ACK] Seq=636 Ack=1245 Win=64240 Len=0 |
| 16 | 1.145439844 | 129.215.32.13 | 172.16.76.155 | HTTP | 662 | HTTP/1.1 200 OK [text/html] |
| 17 | 1.145496842 | 172.16.76.155 | 129.215.32.13 | TCP | 54 | 345612 → 80 [ACK] Seq=1245 Ack=1218 Win=31859 Len=0 |

Packet 14 Details:

- Frame 14: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits) on interface 0
- Ethernet II, Src: Vmware,08:00:02:00:0c:29:0e:08:02, Dst: Vmware,F0:7d:d2:00:50:56:f0:7d:d2
- Internet Protocol Version 4, Src: 172.16.76.155, Dst: 129.215.32.13
- Transmission Control Protocol, Src Port: 345612 (345612), Dst Port: 80 (80), Seq: 636, Ack: 610, Len: 609
- Hypertext Transfer Protocol
- Host: homepages.inf.ed.ac.uk/vr/vn
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0/vr/vn
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8/vr/vn
- Accept-Language: en-US,en;q=0.5/vr/vn
- Accept-Encoding: gzip, deflate/vr/vn
- Referer: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html/vr/vn
- Cookie: _gn=041.3.308514329.1470874824/vr/vn
- Connection: keep-alive/vr/vn
- Upgrade-Insecure-Requests: 1/vr/vn
- Content-Type: application/x-www-form-urlencoded/vr/vn
- Content-Length: 20/vr/vn
- Full request URI: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html

Raw Packet Data (Hex):

```
0010 3a 20 65 05 65 70 2d 61 66 69 76 65 6d 8a 55 79 : keep-a live..Up
```

Raw Packet Data (ASCII):

```
0010 67 72 61 64 05 2d 49 6e 73 65 63 75 72 65 2d 52 : grade-1 secure-k
```

Raw Packet Data (Hex):

```
0020 65 72 75 65 73 74 73 3a 29 33 0a 0a 43 6f 6e 74 : equests: 1..cont
```

Raw Packet Data (ASCII):

```
0020 65 6e 74 2d 54 79 70 65 3a 29 61 70 76 6c 69 63 : ent-type: applic
```

Raw Packet Data (Hex):

```
0030 63 74 69 6f 6e 2f 78 2d 77 77 72 66 6f 72 6d 6d : ation/x-www-form
```

Raw Packet Data (ASCII):

```
0030 2d 75 72 6c 65 63 6f 64 65 64 0a 43 6f 6e 6d : urleenco ded..con
```

Raw Packet Data (Hex):

```
0040 0a 0a 75 65 3d 30 6f 72 74 6f 28 70 77 3d 31 : ..unway ftdpw=1
```

Raw Packet Data (ASCII):

```
0040 32 33 34 35 36 37 38 : 2345678
```

An attacker can **intercept** packets, but also **alter**, **forge** new, and **inject** packets

More complex systems needed...

More complex systems needed...



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



More complex systems needed...



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



Replay attack



$$\xrightarrow{(e,m)}$$



$$\xrightarrow{(e,m)}$$

⋮

$$\xrightarrow{(e,m)}$$



... 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 :(

EDITOR: UK

zdNet Q 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

threat **post** 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

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

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

Example: RSA

A

|

B

|

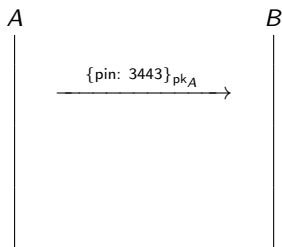
Example of a logical attack

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



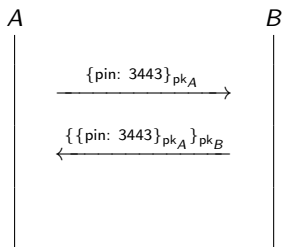
Example of a logical attack

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



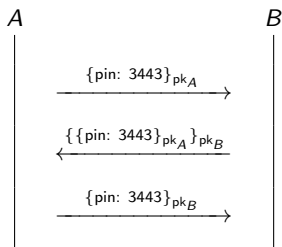
Example of a logical attack

Assume a commutative symmetric encryption scheme

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

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

Example: RSA



since $\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}_{pk_B}\}_{pk_A}$ by commutativity

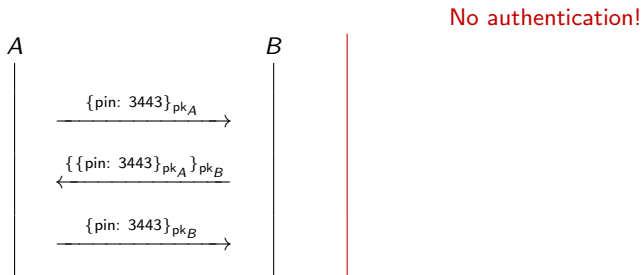
Example of a logical attack

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



since $\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}_{pk_B}\}_{pk_A}$ by commutativity

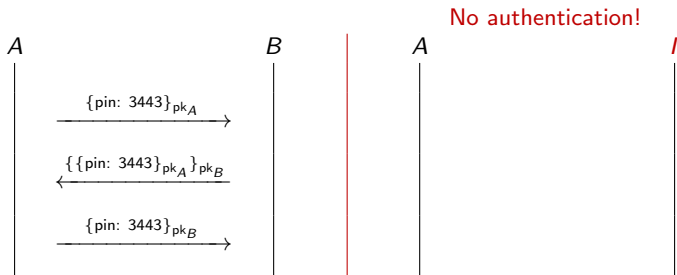
Example of a logical attack

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



since $\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}_{pk_B}\}_{pk_A}$ by commutativity

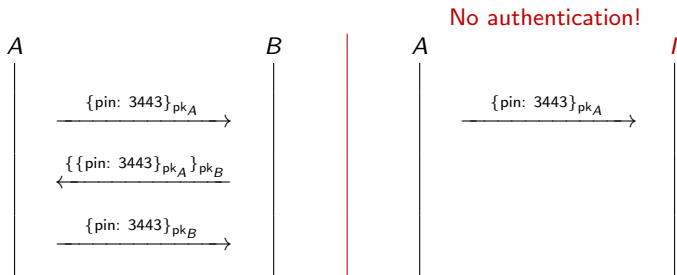
Example of a logical attack

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



since $\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}_{pk_B}\}_{pk_A}$ by commutativity

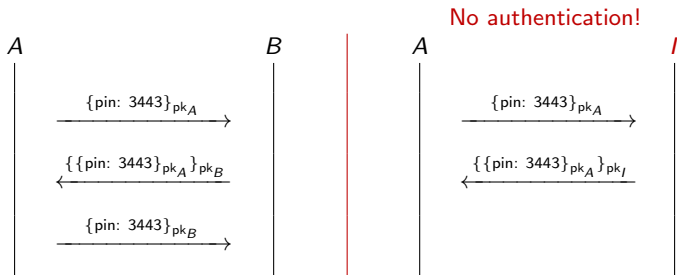
Example of a logical attack

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



since $\{\{\text{pin: 3443}\}_{pk_A}\}_{pk_B} = \{\{\text{pin: 3443}\}_{pk_B}\}_{pk_A}$ by commutativity

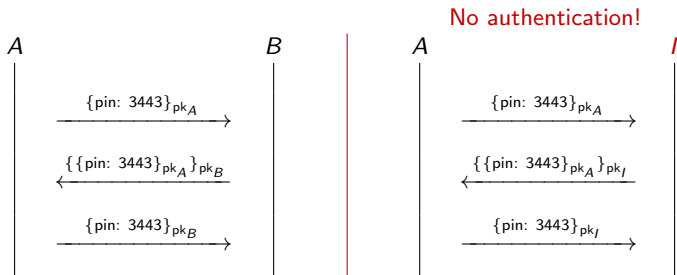
Example of a logical attack

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



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 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
- ~> 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)

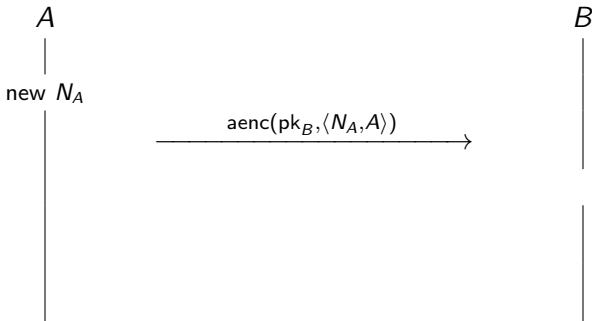
NSPK: authentication and key agreement protocol



[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)

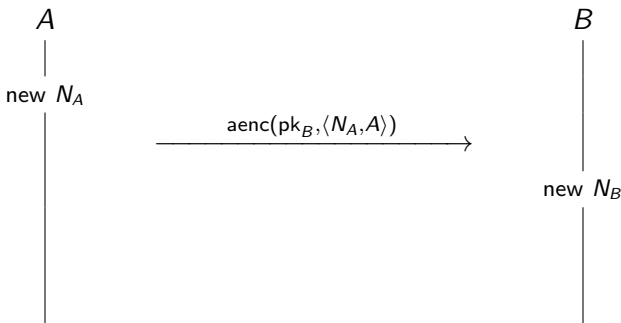
NSPK: authentication and key agreement protocol



[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)

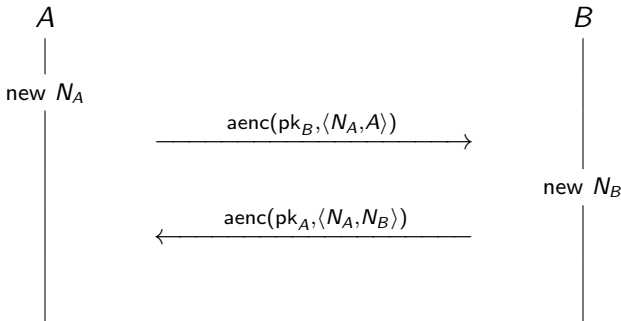
NSPK: authentication and key agreement protocol



[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)

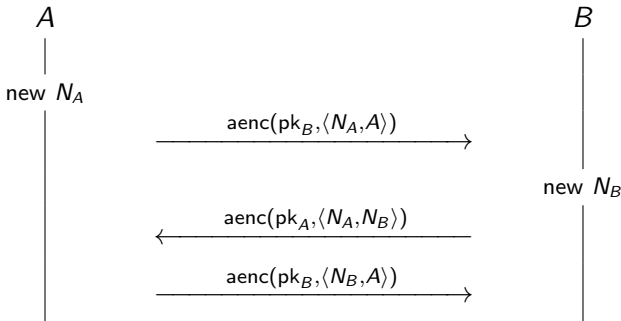
NSPK: authentication and key agreement protocol



[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)

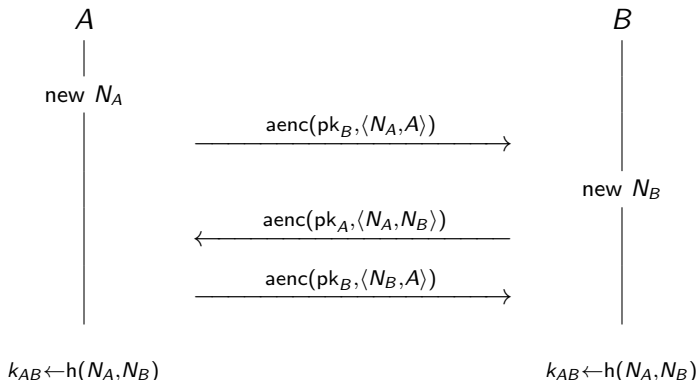
NSPK: authentication and key agreement protocol



[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

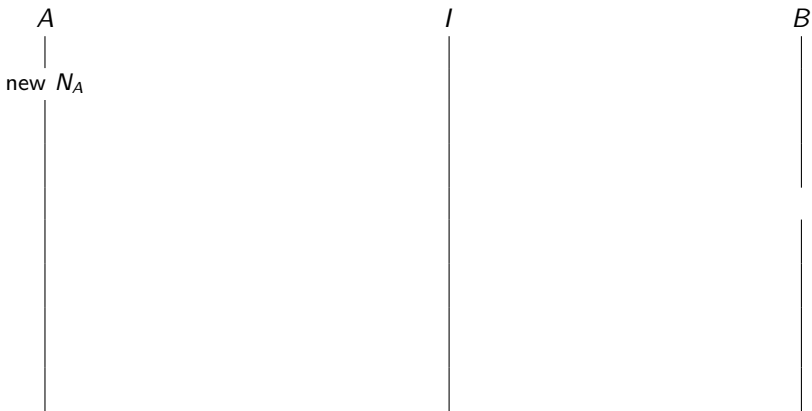
- ▶ **Authentication:** if Alice has completed the protocol, apparently with Bob, then Bob must also have completed the protocol with Alice.
- ▶ **Authentication:** If Bob has completed the protocol, apparently with Alice, then Alice must have completed the protocol with Bob.
- ▶ **Confidentiality:**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

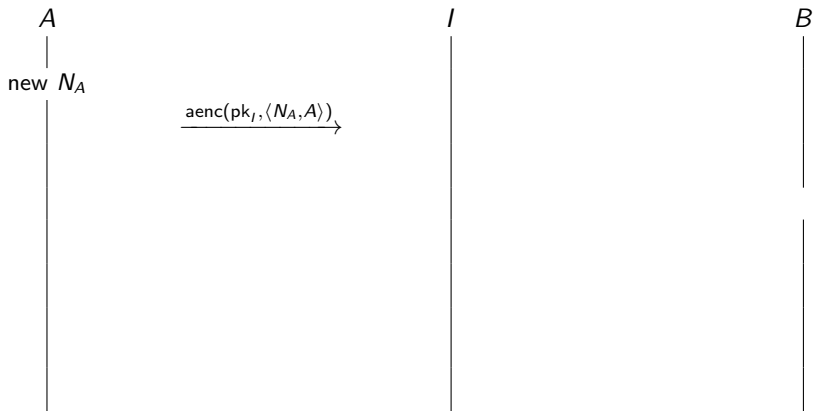
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

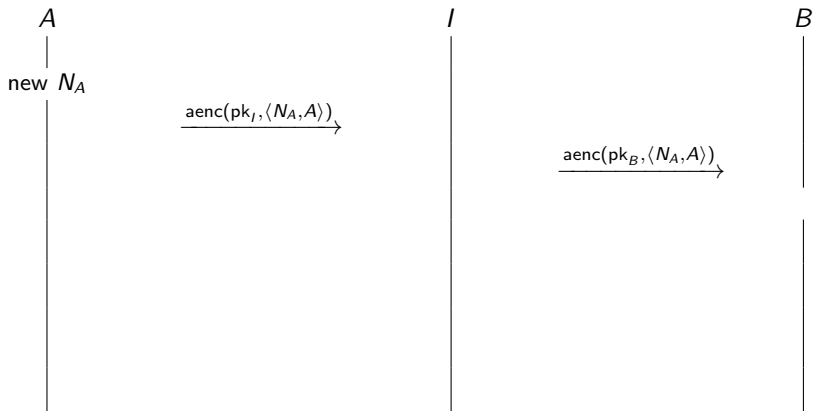
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

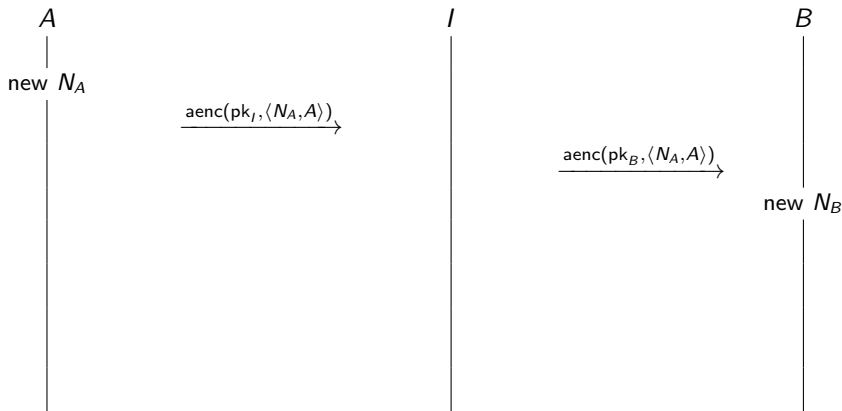
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

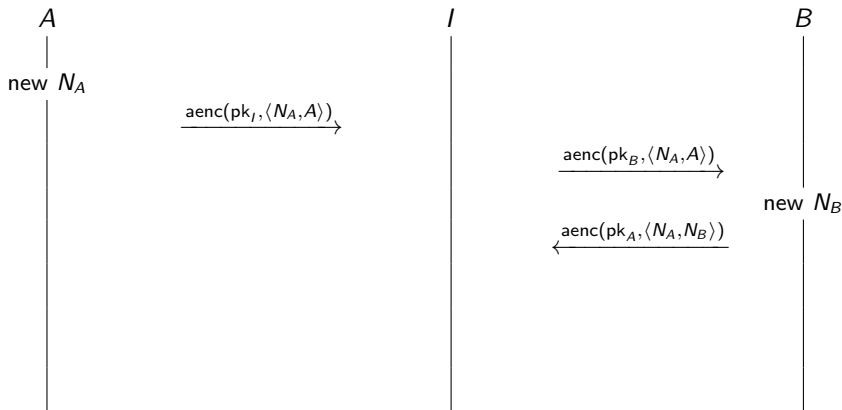
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

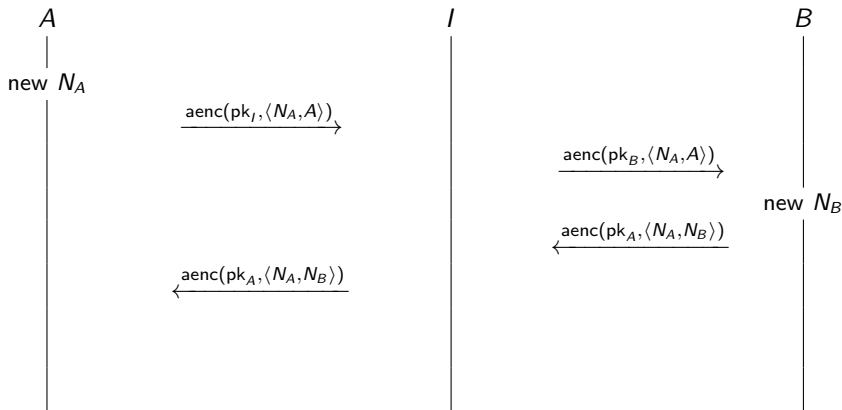
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

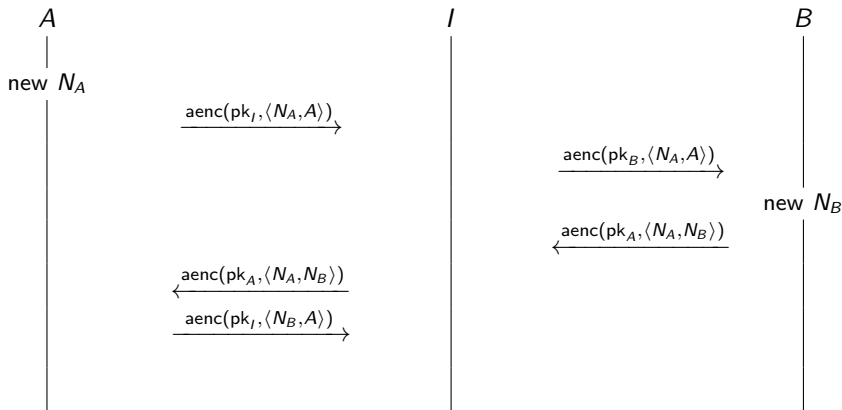
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

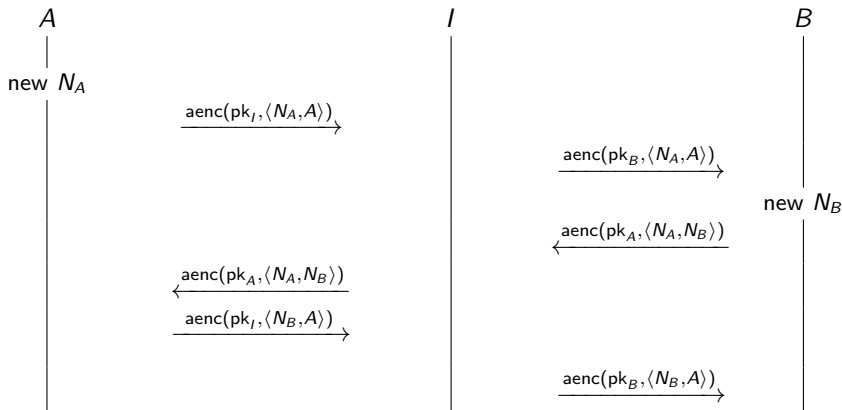
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

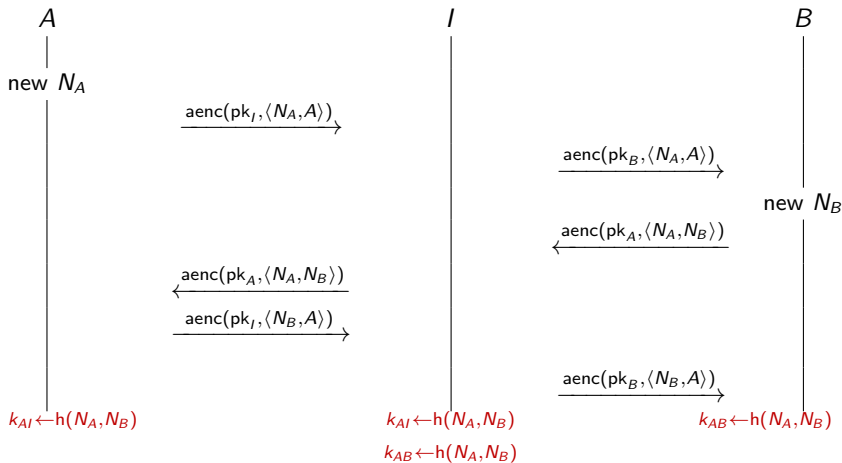
Attack found 17 years after the publication of the NS protocol!!



[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

