

Cryptographic protocols

Myrto Arapinis
School of Informatics
University of Edinburgh

October 17, 2017

Context

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

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

Context

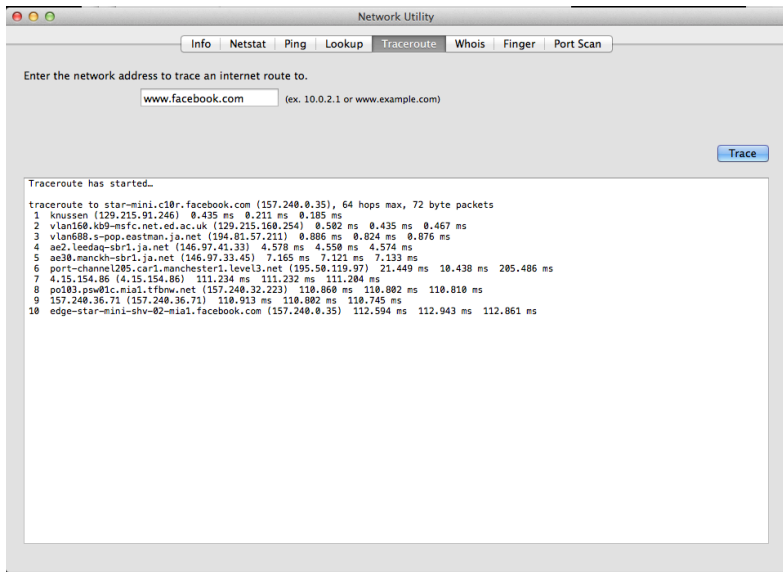
Applications exchanging **sensitive data** over a **public network**:

- ▶ 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)

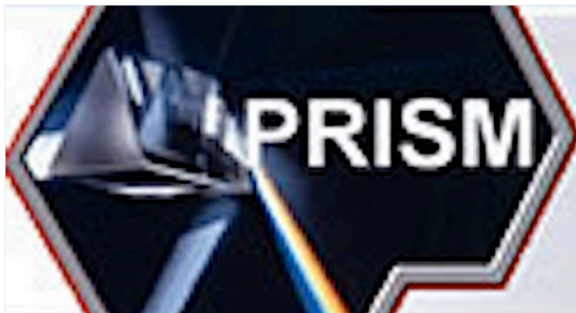


[DATA CENTRE](#) [SOFTWARE](#) [NETWORKS](#) [SECURITY](#) [TRANSFORMATION](#) [DEVOPS](#) [BUSINESS](#) [HARDWARE](#)

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](#)



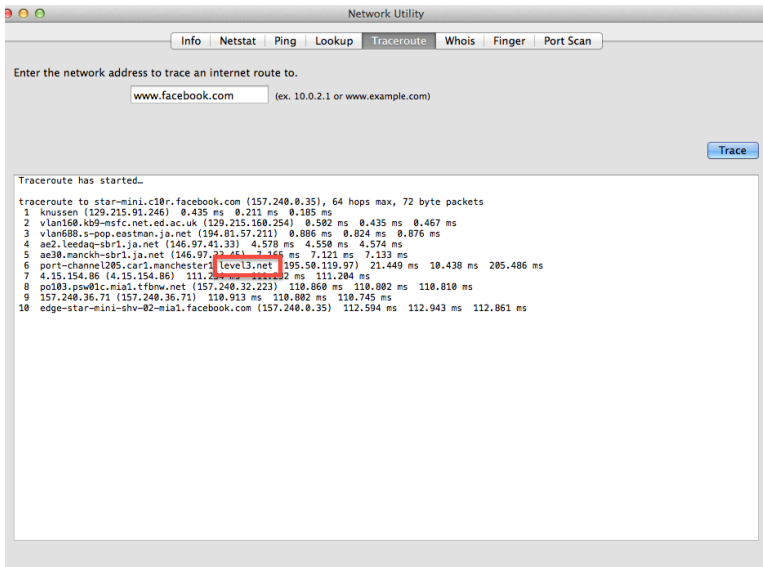
2



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

4 / 20

The attacker controls the network (3)



Network Utility

Info Netstat Ping Lookup **Traceroute** Whois Finger Port Scan

Enter the network address to trace an internet route to.

(ex. 10.0.2.1 or www.example.com)

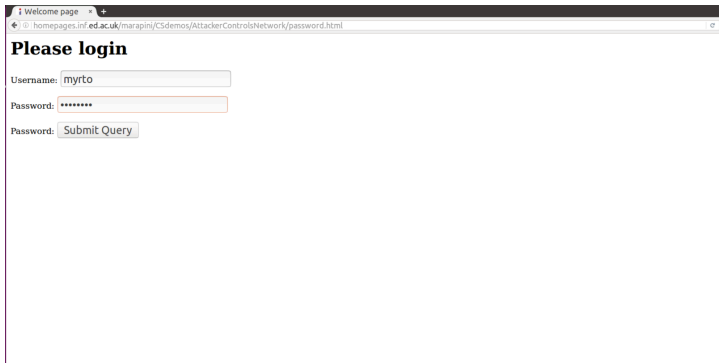
Trace

Traceroute has started.

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

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.psw01c.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)



A screenshot of a web browser window. The address bar shows the URL: `homepages.inf.ed.ac.uk/marapini/C5demos/AttackerControlsNetwork/password.html`. The page title is "Welcome page". The main heading is "Please login". Below the heading, there are three input fields: "Username:" with the text "myrto", "Password:" with masked characters "*****", and another "Password:" field with a "Submit Query" button next to it.

Welcome page

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

Please login

Username: myrto

Password: *****

Password:

All messages can be intercepted by an attacker (2)

The image displays a Wireshark packet capture interface. The top pane shows a list of network packets. Packet 17, at time 15.1998472925, is highlighted. It is an HTTP POST request from 172.16.76.155 to 172.16.76.155. The packet details pane shows the following structure:

- Frame 14: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits) on interface 0
- Ethernet II, Src: Vmware-0e:00:02:00:0c:29:0e:00:02, 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: 36412 (36412), Dst Port: 80 (80), Seq: 636, Ack: 610, Len: 609
- Hypertext Transfer Protocol
- POST /marapini/CSdemos/AttackerControlNetwork/password.html HTTP/1.1
- Host: homepages.inf.ed.ac.uk/vr/n
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0/vr/n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8/vr/n
- Accept-Language: en-US,en;q=0.5/vr/n
- Accept-Encoding: gzip, deflate/vr/n
- Referer: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html/vr/n
- Cookie: _gn=6A1.3.308514329.1470674824/vr/n
- Connection: keep-alive/vr/n
- Upgrade-Insecure-Requests: 1/vr/n
- Content-Type: application/x-www-form-urlencoded/vr/n
- Content-Length: 208/vr/n
- v/r/n
- Full request URI: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html
- len=...cont
- 38 20 65 05 65 70 2d 61 66 69 76 65 6d 08 55 70 : keep-a live..Up
- 0230 07 72 61 64 05 2d 49 6e 73 65 63 75 72 05 2d 52 : grade-In secure-#
- 0230 65 72 75 65 73 74 73 38 29 33 0d 0a 43 6f 6e 74 : equests: 1..cont
- 0240 65 6e 74 2d 54 79 70 65 38 29 61 70 76 6c 69 63 : ent-type: applic
- 0250 63 74 69 6f 6e 2f 78 2d 77 77 72 6d 6f 72 6d : ation/x-ww-form
- 0260 2d 75 72 6c 05 65 6f 64 65 64 0d 0a 43 6f 6e : -urlenco ded..con
- 0270 74 65 6e 74 2d 4c 65 6e 6f 74 65 38 29 32 30 6d : ..unway ftdpw=1
- 0280 32 33 34 35 36 37 3d 38 : 2345678

The bottom status bar indicates: Packets: 17 / Displayed: 17 (100.0%) Profile: Default

All messages can be intercepted by an attacker (2)

The image shows a Wireshark packet capture interface. The top pane displays a list of network packets. Packet 14 is highlighted, showing an HTTP GET request from 172.16.76.155 to 172.16.76.2. The packet details pane on the right shows the structure of the HTTP request, including the request line, headers, and body. The request is for the URL `http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html`. The body of the request contains a form with a text input field and a submit button.

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,08:00:02:00:0c:29:0e:08:02
• Internet Protocol Version 4, Src: 172.16.76.155, Dst: 172.16.76.155
• Transmission Control Protocol, Src Port: 36412 (36412), Dst Port: 80 (80), Seq: 636, Ack: 610, Len: 609
• Hypertext Transfer Protocol

Host: homepages.inf.ed.ac.uk/vr\nUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0/vr\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8/vr\nAccept-Language: en-US,en;q=0.8/vr\nAccept-Encoding: gzip, deflate/vr\nReferer: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html/vr\nCookie: _gn=6a1.3.308514329.1470874824/vr\nConnection: keep-alive/vr\nUpgrade-Insecure-Requests: 1/vr\nContent-Type: application/x-www-form-urlencoded/vr\nContent-Length: 20/vr\n\nFull request URI: http://homepages.inf.ed.ac.uk/marapini/CSdemos/AttackerControlNetwork/password.html/vr\n\nkeep-alive\n38 20 65 05 65 70 2d 61 66 69 76 65 6d 08 55 70 : keep-alive, Up
0220 67 72 61 64 05 2d 49 6e 73 65 63 75 72 05 2d 52 grade-In secure-#
0230 65 72 75 65 73 74 73 38 29 33 08 0a 43 6f 74 e requests: 1, cont
0240 65 6e 74 2d 54 79 70 65 38 20 61 70 76 6c 69 63 ent-Type: applic
0250 63 74 69 6f 6e 2f 78 2d 77 77 72 66 6f 72 6d ation/x- www-form
0260 2d 75 72 6c 65 63 6f 64 65 64 08 0a 43 6f 6c -urlecno ded, con
0270 74 65 6e 74 2d 4c 65 6e 67 74 65 38 20 32 30 6d -urlecno ded, con
0280 08 0a 76 65 3d 30 70 72 74 67 28 70 77 3d 31 : ...unary ftdpw=1
0290 32 33 34 36 37 38 3d

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...



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

Replay attack



$\xrightarrow{(e,m)}$



$\xrightarrow{(e,m)}$

\vdots

$\xrightarrow{(e,m)}$



... 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

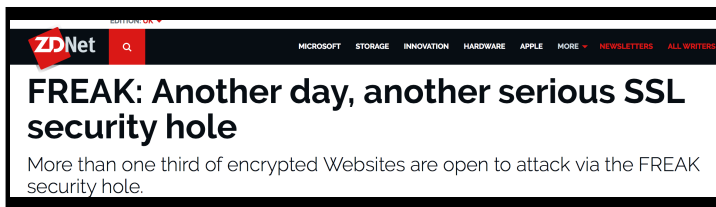
Programs relying on **cryptographic primitives** and whose goal is the establishment of “**secure**” communications.

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...

... and end up in the news :(



EDITORIAL 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

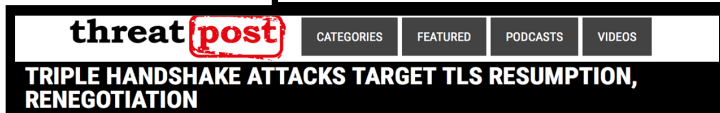


The Register[®]
Biting the hand that feeds IT



Defects in e-passports allow real-time tracking

This threat brought to you by RFID



threat **post**

CATEGORIES FEATURED PODCASTS VIDEOS

TRIPLE HANDSHAKE ATTACKS TARGET TLS RESUMPTION, RENEGOTIATION

Yesterday news :(

threatpost

CATEGORIES

FEATURED

PODCASTS

VIDEOS



[Welcome](#) > [Blog Home](#) > [Privacy](#) > KRACK Attack Devastates Wi-Fi Security



by **Michael Mimoso** Follow @mike_mimoso

October 16, 2017 , 10:16 am

A devastating weakness plagues the WPA2 protocol used to secure all modern Wi-Fi networks, and it can be abused to decrypt traffic from enterprise and consumer networks with varying degrees of difficulty.



Attack published yesterday found after 14 years!!!

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: stream ciphers

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: stream ciphers

A

|

|

B

|

|

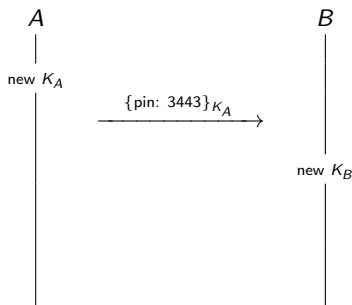
Example of a logical attack

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: stream ciphers



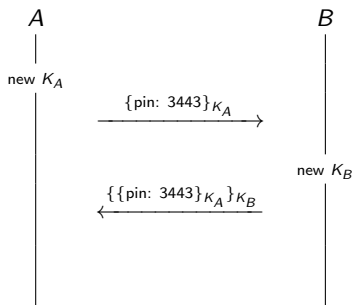
Example of a logical attack

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: stream ciphers



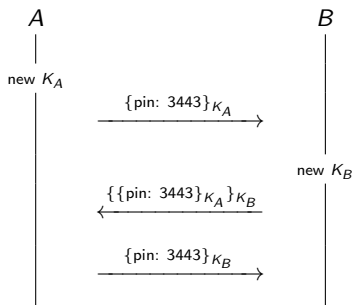
Example of a logical attack

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: stream ciphers



since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ by commutativity

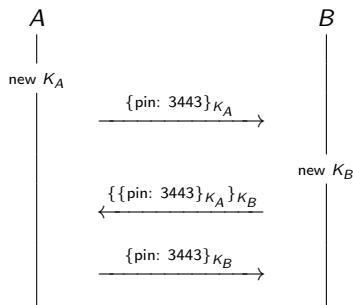
Example of a logical attack

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: stream ciphers



No authentication!

since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ by commutativity

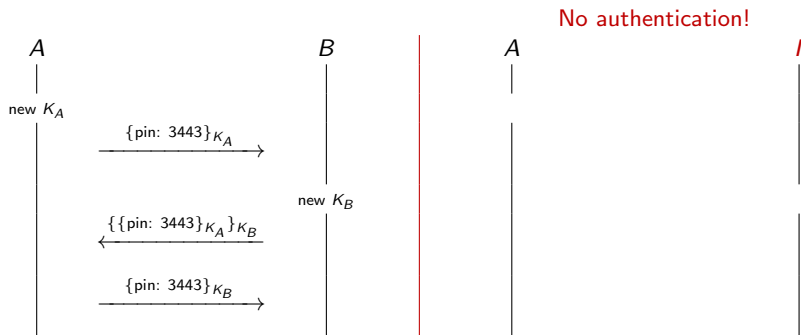
Example of a logical attack

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: stream ciphers



since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ by commutativity

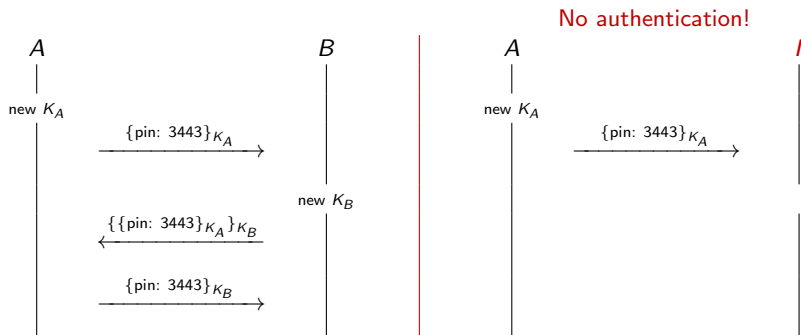
Example of a logical attack

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: stream ciphers



since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ by commutativity

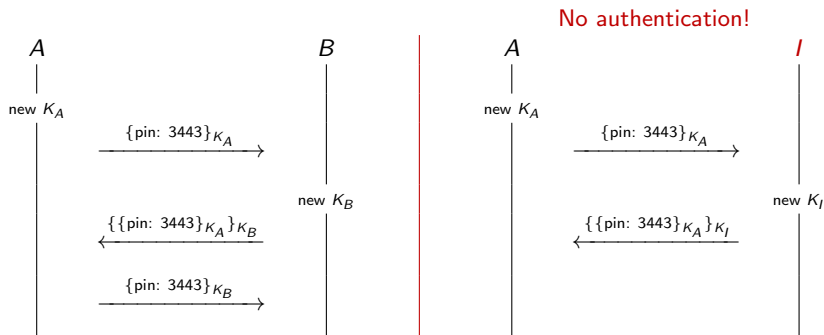
Example of a logical attack

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: stream ciphers



since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ by commutativity

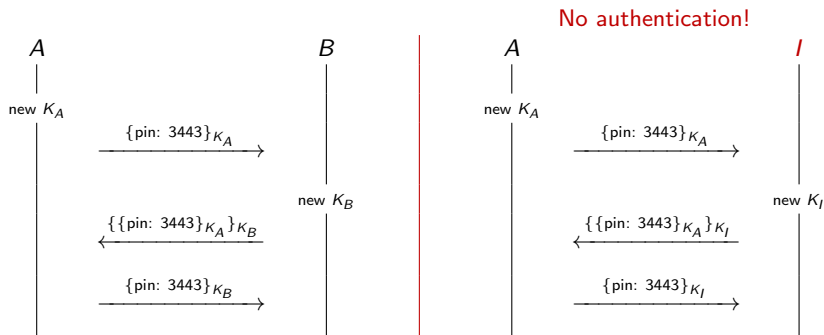
Example of a logical attack

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: stream ciphers



since $\{\{\text{pin: 3443}\}_{K_A}\}_{K_B} = \{\{\text{pin: 3443}\}_{K_B}\}_{K_A}$ 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)

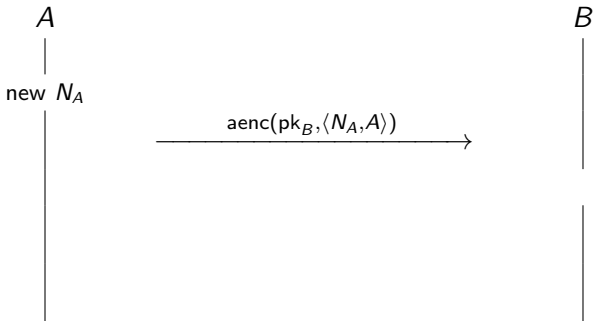
NSPK: authentication and key agreement protocol



[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)

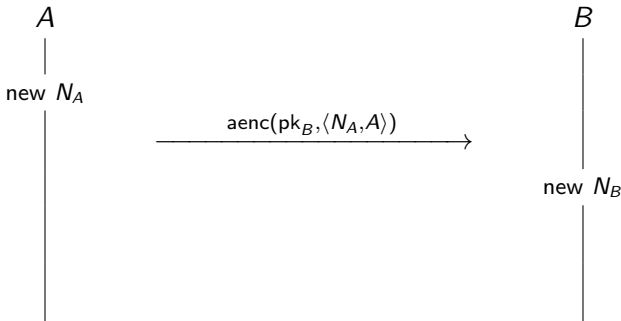
NSPK: authentication and key agreement protocol



[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)

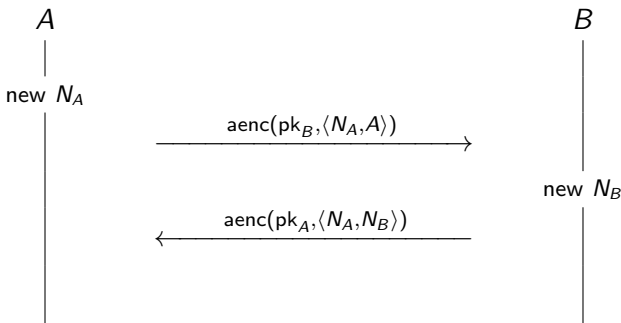
NSPK: authentication and key agreement protocol



[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)

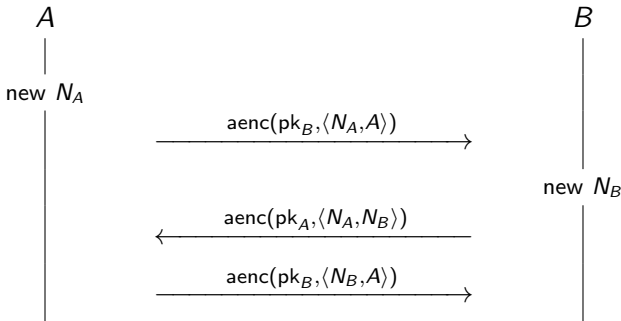
NSPK: authentication and key agreement protocol



[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)

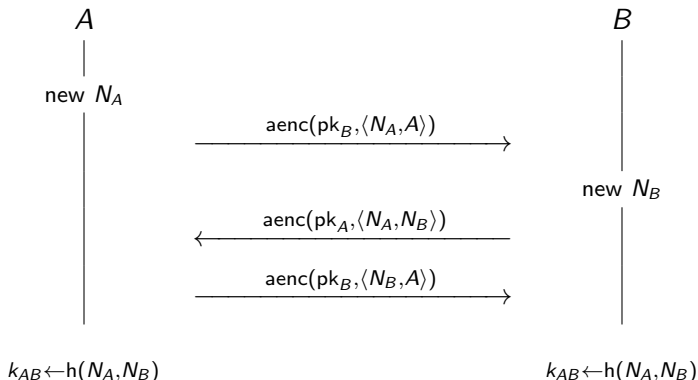
NSPK: authentication and key agreement protocol



[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

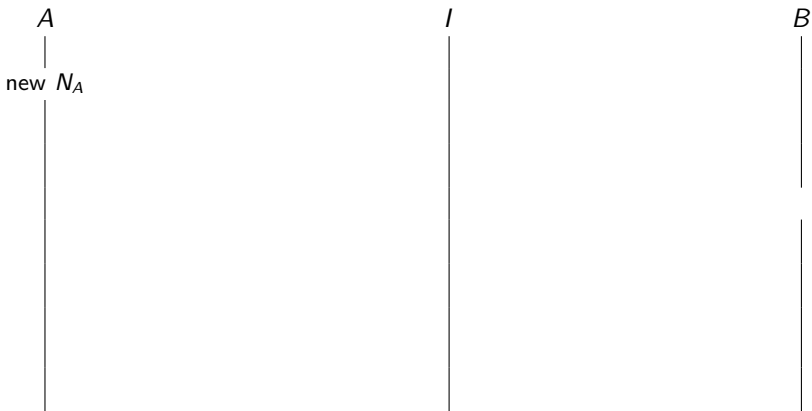
- ▶ **Authentication:** if Alice has completed the protocol, apparently with Bob, then Bob must also have completed the protocol with Alice.
- ▶ **Authentication:** If Bob has completed the protocol, apparently with Alice, then Alice must have completed the protocol with Bob.
- ▶ **Confidentiality:**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

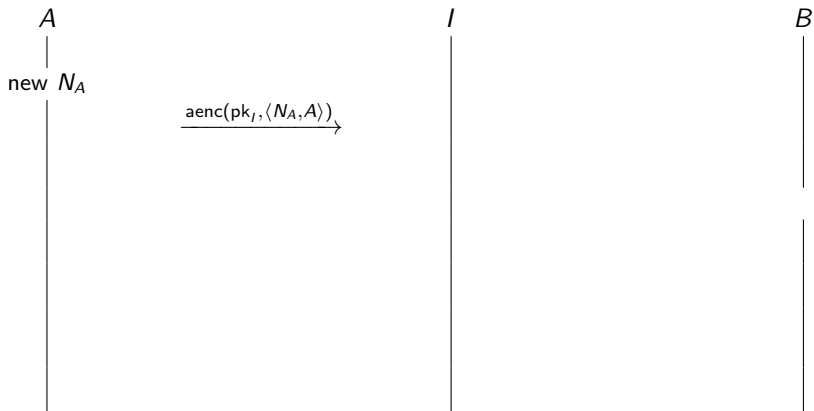
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

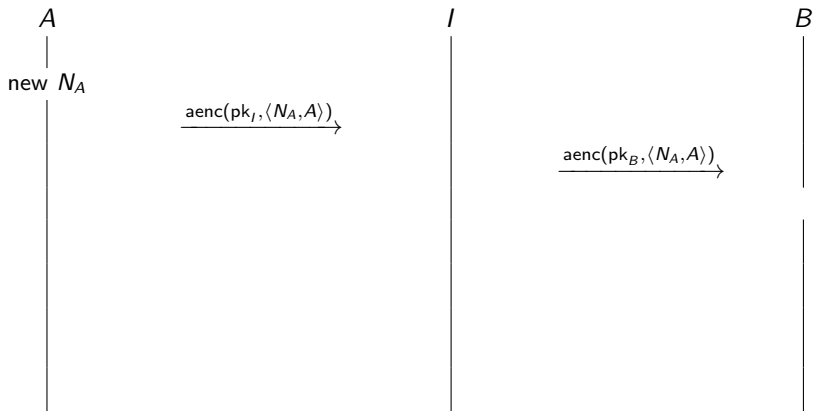
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

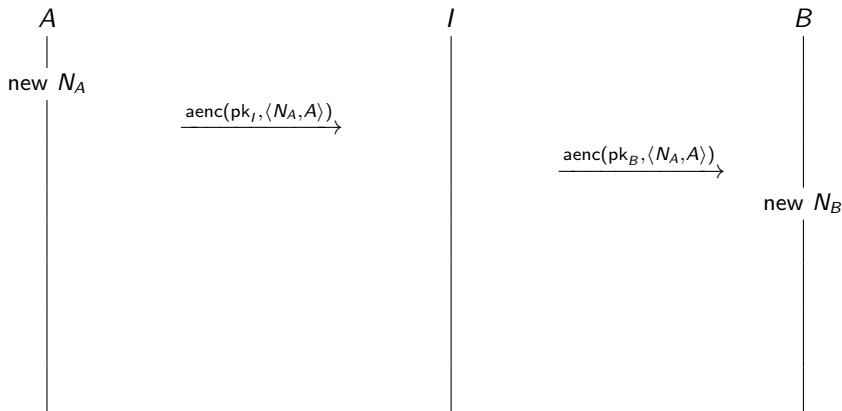
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

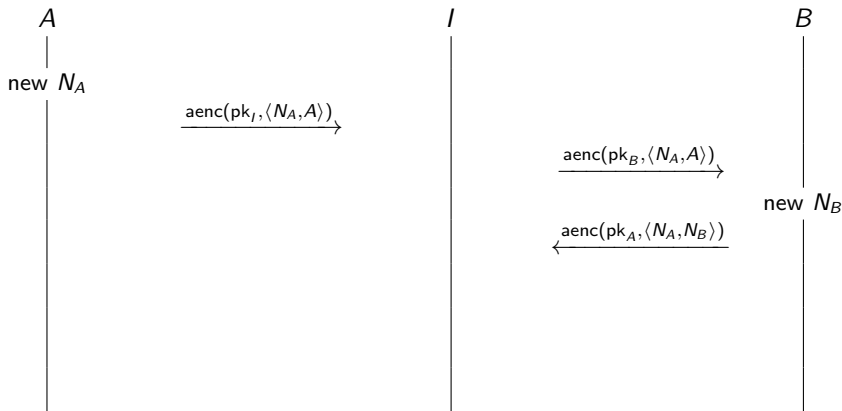
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

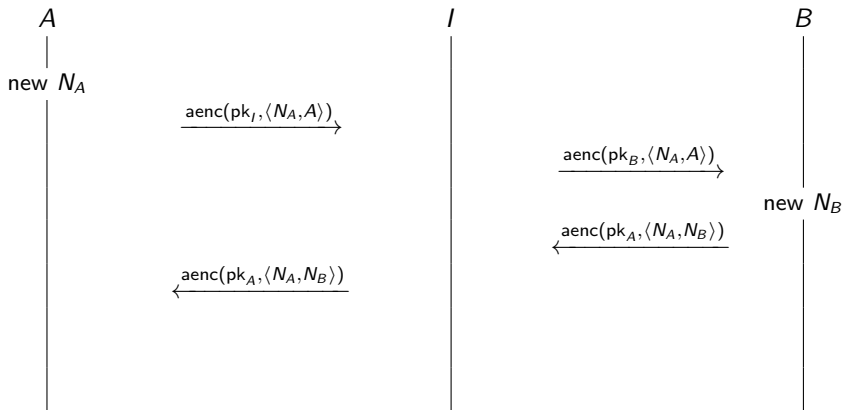
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

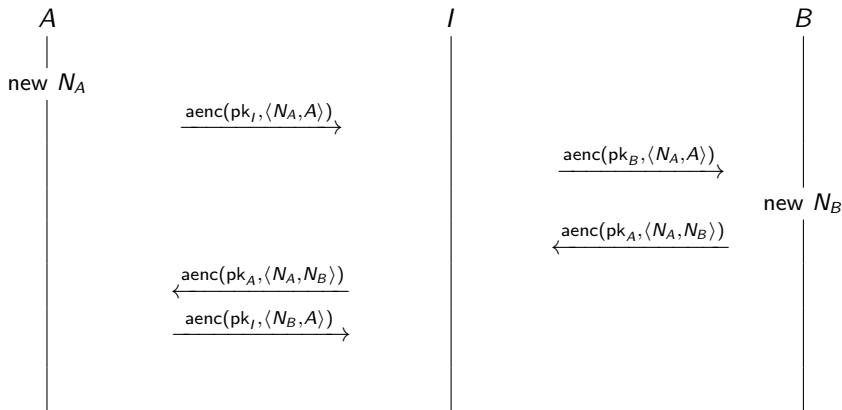
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

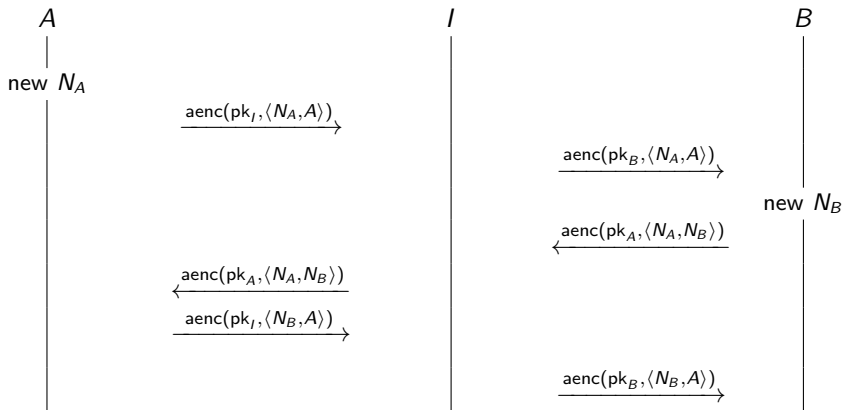
Attack found 17 years after the publication of the NS protocol!!



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

NSPK: Lowe's attack on authentication

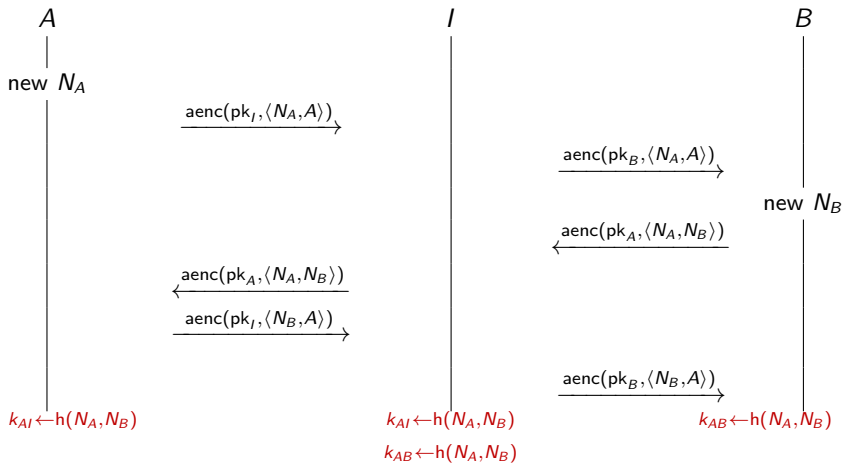
Attack found 17 years after the publication of the NS protocol!!



[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

