



- (51) International Patent Classification:
H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/GB2017/050049
- (22) International Filing Date:
10 January 2017 (10.01.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
1600448.3 11 January 2016 (11.01.2016) GB
- (71) Applicant: **OSIRIUM LIMITED** [GB/GB]; 8 Brewery Court, Theale, Berkshire RG7 5AH (GB).
- (72) Inventor: **HARRIS, Andrew Steven**; Osirium Limited, 8 Brewery Court, Theale, Berkshire RG7 5AH (GB).
- (74) Agent: **MARKS & CLERK LLP**; BLAKE, Stephen, Alpha Tower, Suffolk Street Queensway, Birmingham B1 1TT (GB).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: CONTROLLING ACCESS TO REMOTE DEVICES

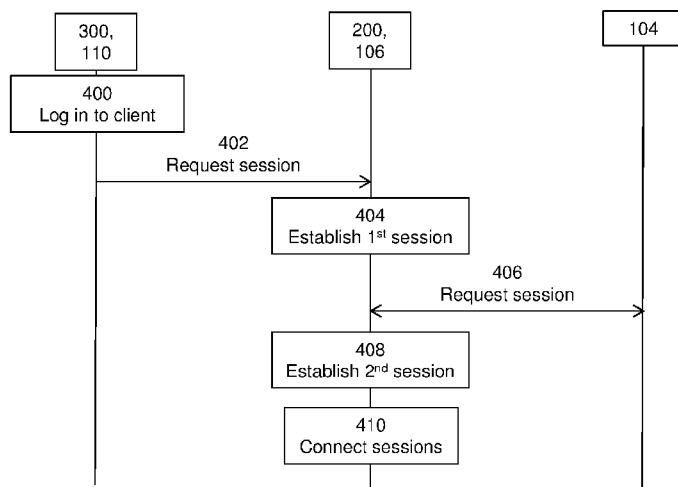


Fig. 4

(57) Abstract: A server (200) for controlling access to a remote device from a user device, the server comprising: a session establisher (214) configured to establish a first session, between a client of the user device and the server, the session establisher being further configured to control a transmitter (202) to transmit remote device credentials to the remote device for establishing a second session, between the server and the remote device, such that the second session is established, and a session connector (216) configured to connect the first and second sessions, such that the client does not have access to the remote device credentials.

CONTROLLING ACCESS TO REMOTE DEVICES

Technical field

5 The invention relates to methods and apparatus for controlling access to a remote device within a computer network from a user device, which may be outside the computer network. In particular, the invention may relate to methods and apparatus for controlling access to the remote device such that credentials for the remote device are not accessible from the user device.

10

Background

15

A computer network within an organisation will typically contain a number of devices, termed remote devices herein, which may include PCs and servers, but also switches, routers, wireless access points, IP cameras, projectors, network attached storage and so on. Each remote device will have a management interface, which may be web-based or may be accessed as one or more applications running on general purpose operating systems such as Windows or Linux. In addition to physical components of a network, a remote device in this context may itself be an application running on a physical component or over the Internet.

20

25

Remote devices may be controlled by users logging in to user or admin accounts from user devices. Some remote devices may provide only a single management user or admin account, while others may allow many accounts with various levels of functionality, or even integrate directly with organisational user directories. Each user or admin account will typically require user credentials for each user attempting to gain access to one or more remote devices.

30

As used herein, the term “user credentials” encompasses any data that may be used to log in to a user or admin account for controlling a device. Accordingly, user credentials may comprise a user ID and/or secure data, such as a text string or password, identifying that user.

35

Where an organisation has many IT staff there arises the issue of managing multiple admin accounts and maintaining an audit trail of which admin user logged on to which

remote device and when. Additionally, network security may be compromised where a user is allowed to access remote device credentials that allow log in to one or more remote devices across the network. Matters are compounded when an organisation wishes to allow external users, outside of the organisation's network, to access remote devices, as the remote device credentials are then required to be in the hands of individuals outside the organisation owning the remote device.

Known solutions may be provided by simply storing remote device credentials in a database. A user may transmit a request to the database and then receive remote device credentials allowing access to one or more remote devices as part of a network administration role. In other, less technological solutions, a user may keep a physical record of remote device credentials for accessing a remote device as part of a network administration role in what may be termed a "run book". In these systems, the user consults the run book to identify remote device credentials allowing access to devices within the computer network.

The known systems introduce security weaknesses into a computer network.

Summary

According to the invention in an aspect, there is provided a server for controlling access to a remote device from a user device, the server comprising: a session establishing means, which may be a session establisher, configured to establish a first session, between a client of the user device and the server, the session establisher being further configured to control a transmitter to transmit remote device credentials to the remote device for establishing a second session, between the server and the remote device, such that the second session is established; and a session controlling means, which may be a session connector, configured to connect the first and second sessions, such that the client does not have access to the remote device credentials.

Optionally, the server further comprises a receiving means, which may be a receiver configured to receive from the client a request to establish the first session, the request comprising user credentials for a user; and a user determining means, which may be a user determiner, configured to determine whether the user is an authorised user based

on the received user credentials, wherein the session establisher is configured to establish the first session in dependence on the user being an authorised user.

Optionally, the user credentials provide two factor authorisation.

5

Optionally, the user determiner is configured to determine whether the user is authorised to access the remote device, and wherein the session establisher is configured to control the transmitter to transmit remote device credentials to the remote device for establishing the second session, in dependence on the user being an authorised user.

10

Optionally, the server further comprises a one instance enforcing means, which may be a one instance enforcer, configured to determine whether there is an existing first session established for the user and, if there is an existing first session, to end the existing first session before establishing the requested first session.

15

Optionally, the first session comprises an encrypted session.

Optionally, the encrypted session is one of a secure shell, SSH, or secure sockets layer, SSL, tunnel.

20

Optionally, the first session comprises a non-encrypted session running within the encrypted session.

25

Optionally, the session establisher is configured to establish the first session with a client in a first network, and to establish the second session with a remote device in a second network.

30

Optionally, the server further comprises a receiver configured to receive from the remote device, in response to the transmitted remote device credentials, session establishment data for establishing the second session, and wherein the session establisher is configured to establish the second session based on the received session establishment data.

Optionally, the session establisher is configured to establish the first session in a first context of an operating system running on the server, and to establish the second session in a second context of the operating system, wherein one of the first or second contexts is unable to access memory associated with the other of the first or second contexts.

Optionally, the session connector is configured to connect the first and second sessions at a socket level.

According to the invention in another aspect, there is provided a system comprising a server as described herein, and a user device comprising the client, the client further comprising: a session establishing means, which may be a session establisher configured to control a transmitter to transmit a request to the server for establishing the first session, the request comprising user credentials for the user.

Optionally, the client further comprises a one instance enforcing means, which may be a one instance enforcer, configured to determine whether there is an existing first session established for the user and, if there is an existing first session, to end the existing first session before controlling the transmitter to transmit the request.

Optionally, the client further comprises a port generating means, which may be a port generator configured to generate an ephemeral port at the user device, wherein the transmitted requested comprises data for establishing the first session via the ephemeral port.

1 Optionally, the client further comprises a session recorder

According to the invention in another aspect, there is provided a method or use on a server for controlling access to a remote device from a user device, the method comprising: establishing, at a session establisher, a first session, between a client of the user device and the server, controlling, by the session establisher, a transmitter to transmit remote device credentials to the remote device for establishing a second session, between the server and the remote device, such that the second session is established; and connecting, by a session connector, the first and second sessions, such that the client does not have access to the remote device credentials.

According to the invention in another aspect, there is provided a computer program comprising instructions which, when executed on at least one processor, cause the at least one processor to carry out a method disclosed herein.

5

According to the invention in another aspect, there is provided a carrier containing the computer program above, wherein the carrier is one of an electronic signal, optical signal, radio signal, or non-transitory computer readable storage medium.

10 **Brief description of the drawings**

Exemplary embodiments of the invention are described herein with reference to the accompanying drawings, in which:

15 Figure 1 is an architecture diagram showing a device network and a workstation network;

Figure 2 shows a schematic diagram of a server;

Figure 3 shows a schematic diagram of a user device; and

20 Figure 4 shows a signalling diagram of a method for controlling access to a remote device from a user device.

Detailed description

25 Generally, disclosed herein are methods and apparatus for controlling access to a remote device from a user device. The remote device may be one of many remote devices owned by an organisation and may provide access to one or more secure elements of the organisation's network. In such cases, it is desirable for a user not to know the remote device credentials that allow access to the remote device. The methods and apparatus disclosed herein allow a user device to access a remote
30 device without revealing the remote device credentials to the user device.

Therefore, methods and apparatus disclosed provide one to one mapping between an authorised user and an authorised session on a remote device.

A goal is to prevent any direct connection to the remote device and to prevent the intercept of any remote device credentials from the user or the authorised user's system. This may be achieved by one or more of a series of indirections and enforcement points that combine to map a session between the authorised user's system and the remote device (for the purposes of system management etc.) via a server.

Exemplary arrangements disclosed comprise a server between a user device and a remote device that may connect a first session established with the user device and a second session established with the remote device such that the user device has access to the remote device. The server may combine networking techniques and mathematical techniques together to increase the degree of separation between the first and second sessions.

In exemplary methods and apparatus, the remote device credentials can never enter the authorised user's system. Therefore, the remote device credentials cannot be:

- Intercepted;
- Key logged;
- RAM Scraped;
- Derived from a reverse hash lookup; or
- Extracted or Coerced from the Authorised User.

Exemplary methods and apparatus may also include 'gear-lever' technology that allows an organisation to move from a 'no-touch' server deployment through several distinct stages to the environment described herein.

Figure 1 shows an architecture diagram of a device network 100 and a workstation network 102. The device network 100 comprises a remote device 104 and a server 106 for controlling access to the remote device 104. In addition, the device network 100 may comprise other systems and/or remote devices 108, which may be in data communications with the remote device 104. The workstation network 102 comprises a user device 110, in this case external to the device network 100.

The user device 110 comprises a client 112. The client 112 is configured to be in data communications with the server 106. The data communications may be via a public network, such as the Internet, and may use Internet Protocol (IP). The client 112 may be accessed by one or more ephemeral ports 114 that are accessible only for a limited amount of time. The ephemeral ports 114 may be established using a “loopback” IP address in the 127.x.x.x range. Using such an IP address means that the data link layer is not used to transmit data between the client 112 of the user device 110 and the server 106. Data communications between the client 112 and the server 106 may make use of the ephemeral ports and/or the loopback IP address. Therefore, any malware installed on the user device is unable to intercept communications between the client 112 and the server 106.

A user may access the client 112 via a system admin tool 116 and optionally the ephemeral port 114.

The server 106 is configured to establish data communications with the client 112 of the user device 110 and with the remote device 104, but is configured to isolate each of those data communication such that remote device credentials are not available to the user device 110. The operation of the server 106 is discussed in greater detail below.

Figure 2 shows a schematic representation of a server 200, which may be a server 106 in the architecture diagram of Figure 1.

The server 200 comprises a transmitter 202 and a receiver 204. The transmitter 202 and receiver 204 may be in data communication with other network entities within the device network 100 and/or the workstation network 102, such as remote devices 104, user devices 110, servers and/or functions in those networks, and are configured to transmit and receive data accordingly.

The server 200 further comprises a memory 206 and a processor 208. The memory 206 may comprise a non-volatile memory and/or a volatile memory. The memory 206 may have a computer program 210 stored therein. The computer program 210 may be configured to undertake the methods disclosed herein. The computer program 210 may be loaded in the memory 206 from a non-transitory computer readable medium 212, on which the computer program is stored. The processor 208 is configured to

undertake one or more of the functions of a session establisher 214, session connector 216, user determiner 218 and one instance enforcer 220, as set out below.

Each of the transmitter 202 and receiver 204, memory 206, processor 208, session
5 establisher 214, session connector 216, user determiner 218 and one instance
enforcer 220 is in data communication with the other features 202, 204, 206, 208, 210,
214, 216, 218, 220 of the server 200. The server 200 can be implemented as a
combination of computer hardware and software. In particular, the session establisher
214, session connector 216, user determiner 218 and one instance enforcer 220 may
10 be implemented as software configured to run on the processor 208. The memory 206
stores the various programs/executable files that are implemented by a processor 208,
and also provides a storage unit for any required data. The programs/executable files
stored in the memory 206, and implemented by the processor 208, can include the
session establisher 214, session connector 216, user determiner 218 and one instance
15 enforcer 220, but are not limited to such.

Figure 3 shows a schematic representation of a user device 300, which may be a user
device 110 in the architecture diagram of Figure 1.

20 The user device 300 comprises a transmitter 302 and a receiver 304. The transmitter
302 and receiver 304 may be in data communication with other network entities within
the device network 100 and/or the workstation network 102, such as the server 106,
UEs, servers and/or functions in those networks and are configured to transmit and
receive data accordingly.

25 The user device 300 further comprises a memory 306 and a processor 308. The
memory 306 may comprise a non-volatile memory and/or a volatile memory. The
memory 306 may have a computer program 310 stored therein. The computer
program 310 may be configured to undertake the methods disclosed herein. The
30 computer program 310 may be loaded in the memory 306 from a non-transitory
computer readable medium 312, on which the computer program is stored. The
processor 308 is configured to undertake one or more of the functions of a client 314,
session establisher 314, one instance enforcer 318, port generator 320 and session
recorder 322, as set out below.

Each of the transmitter 302 and receiver 304, memory 306, processor 308, client 314, session establisher 314, one instance enforcer 318, port generator 320 and session recorder 322 is in data communication with the other features 302, 304, 306, 308, 310, 314, 316, 318, 320, 322 of the user device 300. The user device 300 can be
5 implemented as a combination of computer hardware and software. In particular, the client 314, session establisher 314, one instance enforcer 318, port generator 320 and session recorder 322 may be implemented as software configured to run on the processor 308. The memory 306 stores the various programs/executable files that are implemented by a processor 308, and also provides a storage unit for any required
10 data. The programs/executable files stored in the memory 306, and implemented by the processor 308, can include the client 314, session establisher 314, one instance enforcer 318, port generator 320 and session recorder 322, but are not limited to such.

Figure 4 shows a signalling diagram of a method for controlling access to a remote
15 device 104 by a user device 300, 110 via a server 200, 106.

A user logs in 400 to the client 314 of the user device 300 using the sysadmin tool 116. As part of the log in 400, the user may supply user credentials to the client 314. The user credentials identify the user and allow the authentication of the user, that is, the
20 establishment of whether the user is authorised to access the remote device 104. The user credentials may provide two factor authentication, in that the user needs to be in possession of a token that provides an additional code.

As part of the log in procedure 400, the one instance enforcer 318 may determine
25 whether the user is already logged in to the server 200. This may be done by maintaining a local store of users logged in and/or by data communication with the server 200. If the user is currently logged in then the one instance enforcer 318 logs the current instance of the user out and logs in the user according to the log in credentials just received. This means that users can move from user device to user
30 device without having to log off first. In addition, if the user credentials fall into another individual's hands and that other individual attempts to log in using those credentials, whether for honest or malicious means, the true user is logged out and so is alerted. The breach of security can therefore be rectified.

Further, the log in of the user may be on one of the ephemeral ports 114. That is, the port generator 320 of the client 314 may generate one or more ephemeral ports 114, as set out above. The client 314 may therefore provide the session(s) that is established with the server 200 to users via local ephemeral ports 114 using the 127.x.x.x IP addresses. This means that any scan by a third party of the 127.x.x.x IP addresses will be inconclusive, for example, because of the high number of possible ports onto which the user may be logged on. The client 314 connects the user's tool chain to a 127.x.x.x:Ephemeral port. Opportunistic connections to those ports simply timeout so that any attacker finds no evidence of a session.

10

After the user has logged in to the client 314, the session establisher 316 of the client 314 controls the transmitter 302 to transmit a request 402 to establish a communications session to the server 200. The request may comprise the user credentials.

15

The receiver 204 of the server 200 receives the request. The session establisher 214 of the server 200 establishes a communications session between the client 314 and the server 200. The user determiner 218 of the server 200 may determine whether the user is entitled to access the remote device 104, based on the user credentials in the request. The session establisher 214 may establish the session with the client 314 in dependence on the user credentials identifying the user as being authorised to access the remote device 104. To this end, the server 200 may have access, e.g. the server 200 may store locally, a database of authorised users. Such a database may identify one or more roles that have access to one or more remote device 104 in the device network 100 and may further identify users authorised to act in those roles.

25

The session between the client 314 to the server 200 may be an encrypted session, such as a tunnelled secure shell (SSH) or Secure Sockets Layer (SSL) session. In such arrangements, unsecured protocols such as Telnet are wrapped in an encrypted session, such as SSH or SSL, which prevents 'on the wire' monitoring. The SSH or SSL session may be authenticated against the user's credentials, as previously described.

30

The client 314 may also comprise a session recorder 322 configured to implement session recording. If this session recording is interrupted for any reason, the session recorder may be configured to terminate the session.

5 The session establisher 214 of the server 200 controls the transmitter 202 to transmit remote device credentials for the remote device 104 to the remote device 104. This may be done in dependence on the user being authorised to access the remote device 104, which may be determined based on the user credentials. The transmitted remote device credentials are part of communications 406 between the server 200 and the
10 remote device 104 to set up a session therebetween. In this way, the session establisher 214 establishes a session 408 with the remote device 104 and performs a login to the remote device 104 using the remote device credentials. As shown in Figure 1, the remote device 104 may be on a separate network to the user device 300.

15 In exemplary arrangements, the server 200 may receive from the remote device 104 session establishment data for establishing the second session. The server 200 may also receive from the remote device 104 data instructing a credential change for the remote device 104. Upon receipt of the data instructing a credential change, the session establisher 214 may generate updated credentials for the remote device 104.
20 The updated credentials may be transmitted to the remote device 104 where they may be stored for future session establishment. In this way, no user input is required to update the credentials for logging into the remote device 104.

In exemplary methods and apparatus, the session establisher 214 may establish the
25 sessions 404 and 408 in different contexts of an operating system, for example LINUX, running on the server 106. Memory of one context cannot be accessed by another context, which means that the session 404 between the server 106 and the user device 110 is unable to obtain the remote device login credentials from the session 408 between the server 106 and the remote device 104.

30

The one instance enforcer 220 of the server 200 may also enforce a one instance policy, as set out above. That is, the one instance policy may be implemented at the user device 300 and/or the server 200.

A session connector 216 connects 410 the two established sessions 404, 408, such that the user device 300 has access to the remote device 104. The session connection isolates the remote device credentials from the session established with the user device 300, for example using separate contexts as explained above. The session
5 connector may, for example, connect the sessions 404, 408 at a socket level such that each session is able to request that the other session undertake some task, but is unable to access the memory of the other session.

The methods and apparatus disclosed herein do not act as a 'router' between networks
10 or between the user device 300 and the remote device 104. The methods and apparatus disclosed set up sessions and connect those sessions within the server 200.

As a further step, the remote device 104 could be configured (or fire walled) to accept only network connections from the server 200. In one configuration, the server 200
15 may have previously created a device account and set its privileges based on the required role. In a 'managed' mode there will be a device account created for each authorised user at each role for every profile that contains the authorised users and the remote device. In essence the device account may be specific for the role defined in each profile the authorised user is a member of. In a network of systems, the accounts
20 are specific to those systems and cannot be used to make implicit jumps or file mappings to other systems.

A computer program may be configured to provide any of the above described methods. The computer program may be provided on a computer readable medium.
25 The computer program may be a computer program product. The product may comprise a non-transitory computer usable storage medium. The computer program product may have computer-readable program code embodied in the medium configured to perform the method. The computer program product may be configured to cause at least one processor to perform some or all of the method.

30 Various methods and apparatus are described herein with reference to block diagrams or flowchart illustrations of computer-implemented methods, apparatus (systems and/or devices) and/or computer program products. It is understood that a block of the block diagrams and/or flowchart illustrations, and combinations of blocks in the block
35 diagrams and/or flowchart illustrations, can be implemented by computer program

instructions that are performed by one or more computer circuits. These computer program instructions may be provided to a processor circuit of a general purpose computer circuit, special purpose computer circuit, and/or other programmable data processing circuit to produce a machine, such that the instructions, which execute via the processor of the computer and/or other programmable data processing apparatus, transform and control transistors, values stored in memory locations, and other hardware components within such circuitry to implement the functions/acts specified in the block diagrams and/or flowchart block or blocks, and thereby create means (functionality) and/or structure for implementing the functions/acts specified in the block diagrams and/or flowchart block(s).

Computer program instructions may also be stored in a computer-readable medium that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable medium produce an article of manufacture including instructions which implement the functions/acts specified in the block diagrams and/or flowchart block or blocks.

A tangible, non-transitory computer-readable medium may include an electronic, magnetic, optical, electromagnetic, or semiconductor data storage system, apparatus, or device. More specific examples of the computer-readable medium would include the following: a portable computer diskette, a random access memory (RAM) circuit, a read-only memory (ROM) circuit, an erasable programmable read-only memory (EPROM or Flash memory) circuit, a portable compact disc read-only memory (CD-ROM), and a portable digital video disc read-only memory (DVD/Blu-ray).

The computer program instructions may also be loaded onto a computer and/or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer and/or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the block diagrams and/or flowchart block or blocks.

Accordingly, the invention may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.) that runs on a processor, which may collectively be referred to as "circuitry," "a module" or variants thereof.

- 5 It should also be noted that in some alternate implementations, the functions/acts noted in the blocks may occur out of the order noted in the flowcharts. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved. Moreover, the functionality of a given block of the
- 10 flowcharts and/or block diagrams may be separated into multiple blocks and/or the functionality of two or more blocks of the flowcharts and/or block diagrams may be at least partially integrated. Finally, other blocks may be added/inserted between the blocks that are illustrated.
- 15 The skilled person will be able to envisage other embodiments without departing from the scope of the appended claims.

CLAIMS:

1. A server for controlling access to a remote device from a user device, the server comprising:

5 a session establisher configured to establish a first session, between a client of the user device and the server,

the session establisher being further configured to control a transmitter to transmit remote device credentials to the remote device for establishing a second session, between the server and the remote device, such that the second session is
10 established; and

a session connector configured to connect the first and second sessions, such that the client does not have access to the remote device credentials.

2. A server according to claim 1, further comprising:

15 a receiver configured to receive from the client a request to establish the first session, the request comprising user credentials for a user; and

a user determiner configured to determine whether the user is an authorised user based on the received user credentials,

wherein the session establisher is configured to establish the first session in
20 dependence on the user being an authorised user.

3. A server according to claim 2, wherein the user credentials provide two factor authorisation.

25 4. A server according to claim 2 or 3, wherein the user determiner is configured to determine whether the user is authorised to access the remote device,

and wherein the session establisher is configured to control the transmitter to transmit remote device credentials to the remote device for establishing the second session, in dependence on the user being an authorised user.

30

5. A server according to any of claims 2 to 4, further comprising a one instance enforcer configured to determine whether there is an existing first session established for the user and, if there is an existing first session, to end the existing first session before establishing the requested first session.

35

6. A server according to any preceding claim, wherein the first session comprises an encrypted session.

5 7. A server according to claim 6, wherein the encrypted session is one of a secure shell, SSH, or secure sockets layer, SSL, tunnel.

8. A server according to claim 7, wherein the first session comprises a non-encrypted session running within the encrypted session.

10 9. A server according to any preceding claim, wherein the session establisher is configured to establish the first session with a client in a first network, and to establish the second session with a remote device in a second network.

15 10. A server according to any preceding claim, further comprising a receiver configured to receive from the remote device, in response to the transmitted remote device credentials, session establishment data for establishing the second session, and wherein the session establisher is configured to establish the second session based on the received session establishment data.

20 11. A server according to any preceding claim, wherein the session establisher is configured to establish the first session in a first context of an operating system running on the server, and to establish the second session in a second context of the operating system, wherein one of the first or second contexts is unable to access memory associated with the other of the first or second contexts.

25

12. A server according to claim 11, wherein the session connector is configured to connect the first and second sessions at a socket level.

30 13. A system comprising a server according to any preceding claim, and a user device comprising the client, the client further comprising:

a session establisher configured to control a transmitter to transmit a request to the server for establishing the first session, the request comprising user credentials for the user.

14. A system according to claim 13, wherein the client further comprises a one instance enforcer configured to determine whether there is an existing first session established for the user and, if there is an existing first session, to end the existing first session before controlling the transmitter to transmit the request.

5

15. A system according to claim 13 or 14, wherein the client further comprises a port generator configured to generate an ephemeral port at the user device,
wherein the transmitted requested comprises data for establishing the first session via the ephemeral port.

10

16. A system according to any of claims 13 to 15, wherein the client further comprises a session recorder configured to record data relating to the first session.

15

17. A method or use on a server for controlling access to a remote device from a user device, the method comprising:

establishing, at a session establisher, a first session, between a client of the user device and the server,

controlling, by the session establisher, a transmitter to transmit remote device credentials to the remote device for establishing a second session, between the server and the remote device, such that the second session is established; and

20

connecting, by a session connector, the first and second sessions, such that the client does not have access to the remote device credentials.

25

18. A computer program comprising instructions which, when executed on at least one processor, cause the at least one processor to carry out the method according to claim 17.

30

19. A carrier containing the computer program of claim 18, wherein the carrier is one of an electronic signal, optical signal, radio signal, or non-transitory computer readable storage medium.

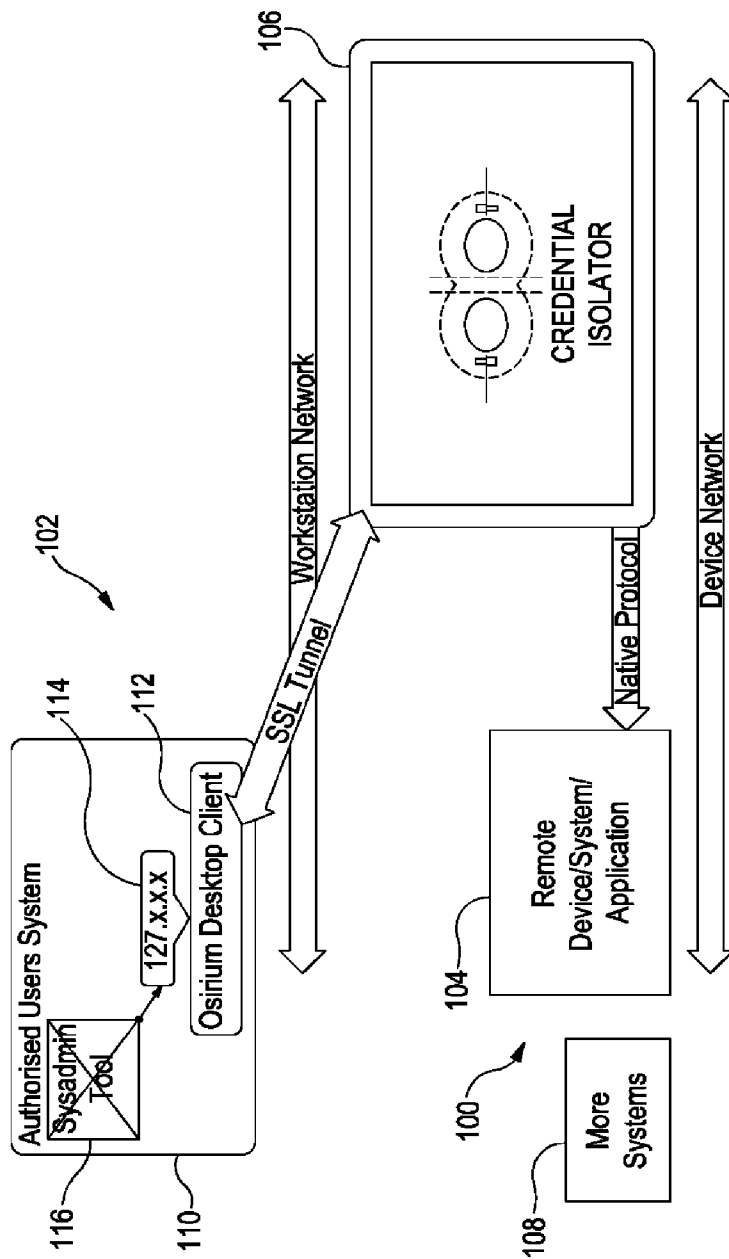


Fig. 1

2/3

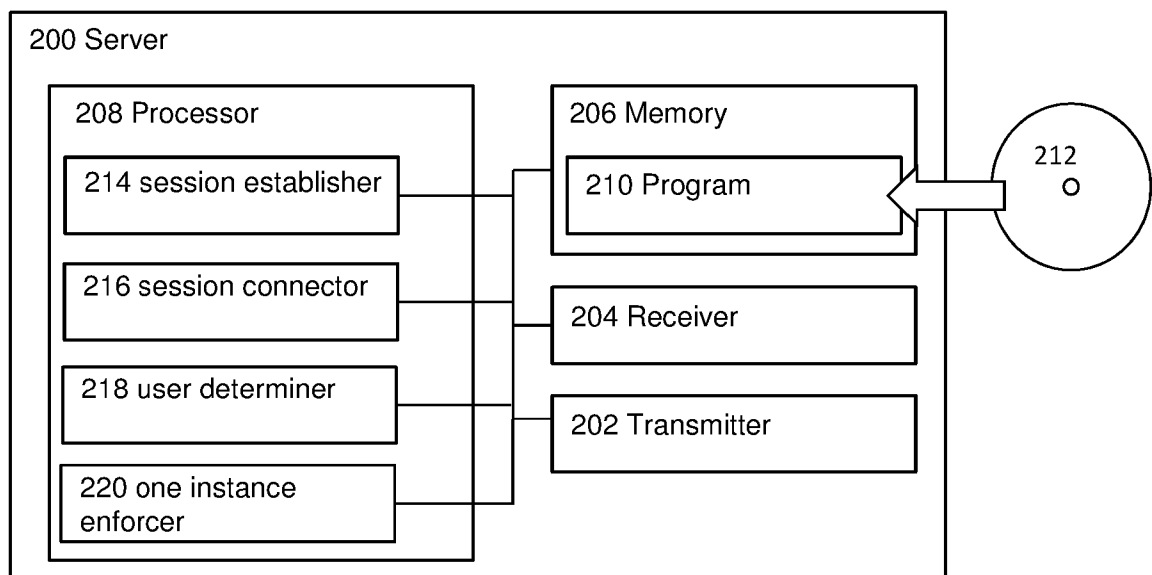


Fig. 2

3/3

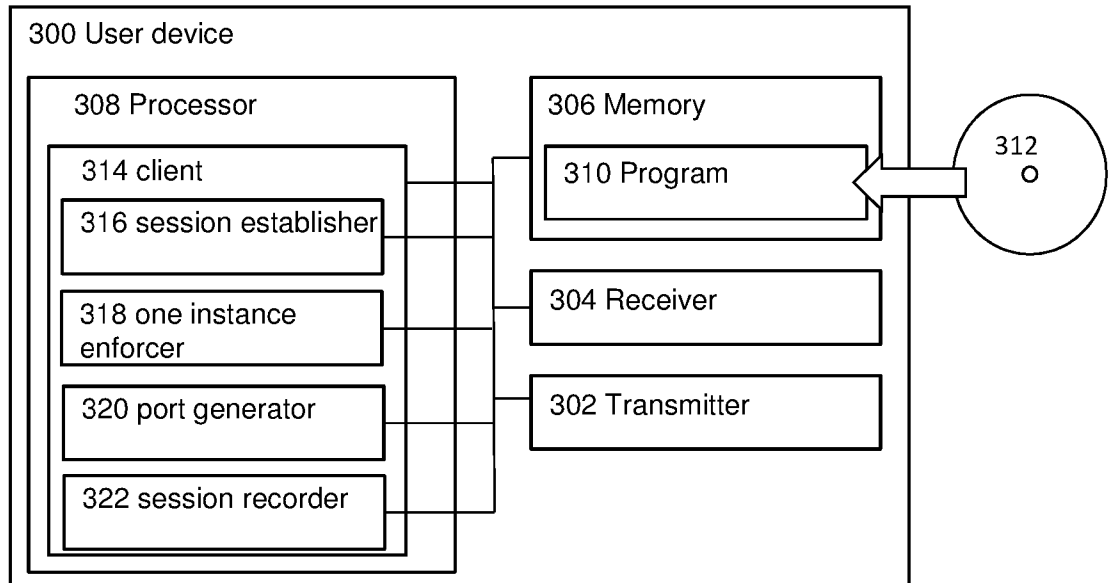


Fig. 3

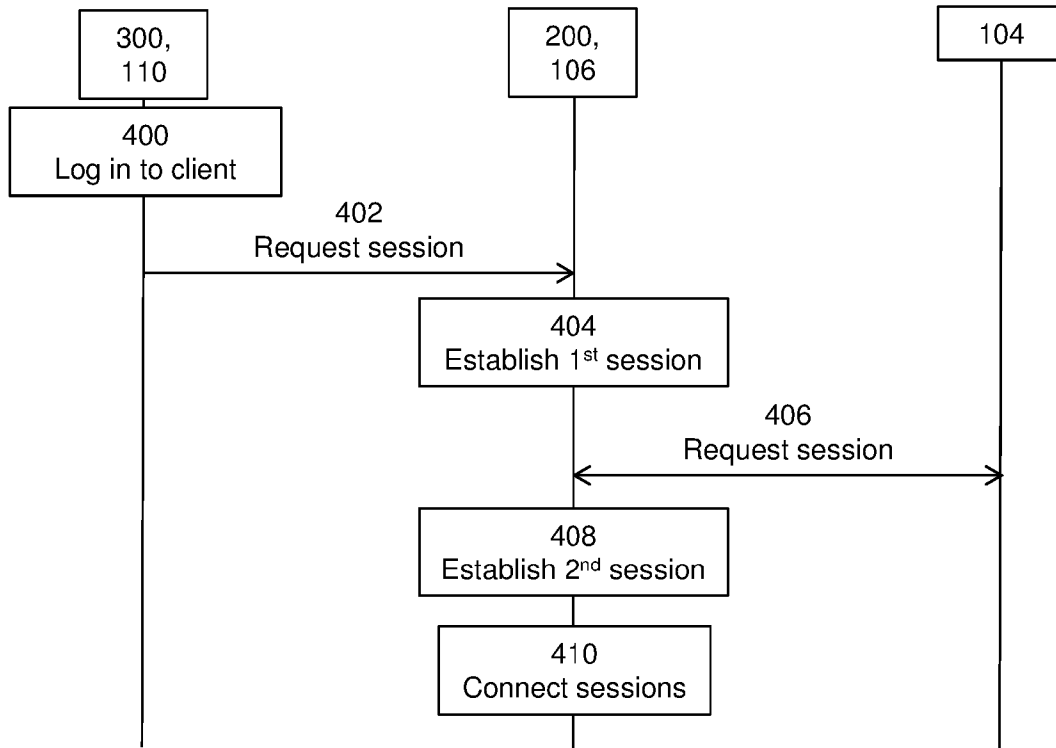


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/GB2017/050049

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L29/06
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/289830 A1 (LEMASTER ROBERT K [US] ET AL) 25 September 2014 (2014-09-25) paragraph [0015] paragraph [0088] claim 3 figures 1,3 paragraph [0047] paragraph [0035] paragraph [0053]	1-19
X	US 2015/271162 A1 (DULKIN ANDREY [IL] ET AL) 24 September 2015 (2015-09-24) paragraph [0001]; figure 1 paragraph [0011] paragraph [0079] paragraph [0081] paragraph [0083] - paragraph [0084] paragraph [0104] - paragraph [0107] ----- -/-	1-19



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

9 March 2017

Date of mailing of the international search report

20/03/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Medvesan, Oana

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2017/050049

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 274 002 A2 (SEIKO EPSON CORP [JP]) 8 January 2003 (2003-01-08) figure 11 paragraph [0014] paragraph [0012] paragraph [0010] -----	1-19
A	US 2011/296510 A1 (HATLELID KRISTJAN E [US] ET AL) 1 December 2011 (2011-12-01) abstract; figure 1 -----	1-19
A	US 2010/058064 A1 (KIROVSKI DARKO [US] ET AL) 4 March 2010 (2010-03-04) abstract; figure 1 -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2017/050049

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014289830	A1	25-09-2014	NONE
US 2015271162	A1	24-09-2015	NONE
EP 1274002	A2	08-01-2003	CN 1402117 A 12-03-2003
		EP 1274002	A2 08-01-2003
		JP 3888452	B2 07-03-2007
		JP 2003084931	A 20-03-2003
		US 2003002077	A1 02-01-2003
		US 2007076252	A1 05-04-2007
		US 2007076253	A1 05-04-2007
US 2011296510	A1	01-12-2011	NONE
US 2010058064	A1	04-03-2010	NONE