

[0095] Computer room 1220 may include one or more operator consoles or other host devices that are configured for communication with SBG server 1230. Such host devices may be provided with software, hardware and/or firmware for implementing various aspects of the invention; many of these aspects involve controlling SBG server 1230. However, such host devices need not be located within computer room 1220. Wired host device 1260 (which is a laptop computer in this example) and wireless host device (which is a PDA in this example) may be located elsewhere in gaming establishment 1205 or at a remote location.

[0096] Arbiter 133 may be implemented, for example, via software that is running on a server or another networked device. Arbiter 133 serves as an intermediary between different devices on the network. Some implementations of Arbiter 133 are described in United States patent application Ser. No. 10/948,387, entitled "Methods And Apparatus For Negotiating Communications Within A Gaming Network" and filed Sep. 23, 2004 (the "Arbiter Application"), which is incorporated herein by reference and for all purposes. In some preferred implementations, Arbiter 133 is a repository for the configuration information required for communication between devices on the gaming network (and, in some implementations, devices outside the gaming network). Although Arbiter 133 can be implemented in various ways, one exemplary implementation is discussed in the following paragraphs.

[0097] FIG. 9 is a block diagram of a simplified communication topology between a gaming unit 21, the network computer 23 and the Arbiter 133. Although only one gaming unit 21, one network computer 23 and one Arbiter 133 are shown in FIG. 9, it should be understood that the following examples may be applicable to different types of network gaming devices within the gaming network 12 beyond the gaming unit 21 and the network computer 23, and may include different numbers of network computers, gaming security arbiters and gaming units. For example, a single Arbiter 133 may be used for secure communications among a plurality of network computers 23 and tens, hundreds or thousands of gaming units 21. Likewise, multiple gaming security arbiters 46 may be utilized for improved performance and other scalability factors.

[0098] Referring to FIG. 9, the Arbiter 133 may include an arbiter controller 121 that may comprise a program memory 122, a microcontroller or microprocessor (MP) 124, a random-access memory (RAM) 126 and an input/output (I/O) circuit 128, all of which may be interconnected via an address/data bus 129. The network computer 23 may also include a controller 131 that may comprise a program memory 132, a microcontroller or microprocessor (MP) 134, a random-access memory (RAM) 136 and an input/output (I/O) circuit 138, all of which may be interconnected via an address/data bus 139. It should be appreciated that although the Arbiter 133 and the network computer 23 are each shown with only one microprocessor 124, 134, the controllers 121, 131 may each include multiple microprocessors 124, 134. Similarly, the memory of the controllers 121, 131 may include multiple RAMs 126, 136 and multiple program memories 122, 132. Although the I/O circuits 128, 138 are each shown as a single block, it should be appreciated that the I/O circuits 128, 138 may include a number of different types of I/O circuits. The RAMs 124, 134 and program memories

122, 132 may be implemented as semiconductor memories, magnetically readable memories, and/or optically readable memories, for example.

[0099] Although the program memories 122, 132 are shown in FIG. 9 as read-only memories (ROM) 122, 132, the program memories of the controllers 121, 131 may be a read/write or alterable memory, such as a hard disk. In the event a hard disk is used as a program memory, the address/data buses 129, 139 shown schematically in FIG. 9 may each comprise multiple address/data buses, which may be of different types, and there may be an I/O circuit disposed between the address/data buses.

[0100] As shown in FIG. 9, the gaming unit 21 may be operatively coupled to the network computer 23 via the data link 25. The gaming unit 21 may also be operatively coupled to the Arbiter 133 via the data link 47, and the network computer 23 may likewise be operatively coupled to the Arbiter 133 via the data link 47. Communications between the gaming unit 21 and the network computer 23 may involve different information types of varying levels of sensitivity resulting in varying levels of encryption techniques depending on the sensitivity of the information. For example, communications such as drink orders and statistical information may be considered less sensitive. A drink order or statistical information may remain encrypted, although with moderately secure encryption techniques, such as RC4, resulting in less processing power and less time for encryption. On the other hand, financial information (e.g., account information, winnings, etc.), game download information (e.g., game software and game licensing information) and personal information (e.g., social security number, personal preferences, etc.) may be encrypted with stronger encryption techniques such as DES or 3-DES to provide increased security.

[0101] As disclosed in further detail in the Arbiter Application, the Arbiter 133 may verify the authenticity of each network gaming device. The Arbiter 133 may receive a request for a communication session from a network device. For ease of explanation, the requesting network device may be referred to as the client, and the requested network device may be referred to as the host. The client may be any device on the network 12 and the request may be for a communication session with any other network device. The client may specify the host, or the gaming security arbiter may select the host based on the request and based on information about the client and potential hosts. The Arbiter 133 may provide encryption keys (session keys) for the communication session to the client via the secure communication channel. Either the host and/or the session key may be provided in response to the request, or may have been previously provided. The client may contact the host to initiate the communication session. The host may then contact the Arbiter 133 to determine the authenticity of the client. The Arbiter 133 may provide affirmation (or lack thereof) of the authenticity of the client to the host and provide a corresponding session key, in response to which the network devices may initiate the communication session directly with each other using the session keys to encrypt and decrypt messages.

[0102] Alternatively, upon receiving a request for a communication session, the Arbiter 133 may contact the host regarding the request and provide corresponding session keys to both the client and the host. The Arbiter 133 may then initiate either the client or the host to begin their communication session. In turn, the client and host may begin the communication session directly with each other using the