REMARKS

Status of the Claims

Claims 1-31 were pending in the application and rejected in the Office Action of February 6, 2014. By this Amendment, Applicant has amended independent claims 1, 27, and 31, and has amended dependent claims 2-9, 11, 13, 16, 19-22, 24, 26, and 28-30, without prejudice or disclaimer of the subject matter contained therein. Furthermore, Applicant has added new claims 33 and 34. The amendments do not introduce new matter. Upon entry of the amendments, claims 1-31, 33, and 34, will be pending. Applicant respectfully requests entry of this Response and favorable reconsideration of the application in view of the amendments and the remarks below.

Rejections under 35 U.S.C. § 101

Claims 1 and 27 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter because claim 1 fails to specify whether it encompasses both software and hardware or software only, and claim 27 recites steps which a person can implement. In response, Applicant has amended independent claims 1 and 27.

Claim 1 is herein amended to specify:

> Apparatus including one or more computer processors configured pursuant to programming code in a non-transient computer readable memory…

The tangible machine elements amended therein are supported by, e.g., paragraphs [0026], [0088], and [0089], of the published application.

Claim 27 is also herein amended to specify that the claim is directed to:

> A computer-implemented method, the method being performed by a computer system having one or more computer processors configured pursuant to programming code in a non-transient computer readable memory…

As amended independent claims 1 and 27 recite specific machine elements to sufficiently tie the subject matter expressed therein to a particular machine. Thus, the applicant respectfully submits that the rejections of independent claims 1 and 27 under 35 U.S.C. § 101 have been overcome.

With regard to § 101, Applicant notes that the dependent claims add elements that further define patent-eligible subject matter. For example, claims 26, 33, and 34, are directed to at least two modules performing specific functions and having a specific relationship to each other.

Rejections under 35 U.S.C. §§ 102

Claims 1-3, 24, and 27-31, are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. 2002/0188870 to Gong ("Gong"). Applicant respectfully traverses the rejections for the reasons noted below.

Independent Claims 1, 27, and 31

Without conceding to positions in the Office Action and for the sole purpose of advancing prosecution, Applicant has currently amended claim 1 to specify that the apparatus is configured to *"...predict future threat activity based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate."* Applicant has also currently amended claim 27 to recite "*...predicting future threat activity based on stochastic modelling of past observed threat events capable of affecting one computer network in which a plurality of systems operate.*" Furthermore, currently amended claim 31 states that the computer readable medium comprises a computer program which when executed causes the computer system to "*...predict future threat activity based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate.*" Basis for the amendments may be found throughout the application as originally filed. Specifically, concerning the amendments specifying the predicted threats are "future" threats, paragraphs [0048] and [0049], for example, disclose:

> [0048] The degree to which an organisation **will be** affected by a successful attack depends on a number of factors, such as the number of IT systems 30 (FIG. 3) affected by the attack and the

> number of operational processes 31 (FIG. 3) relying on the affected IT systems 30 (FIG. 3).
>
> [0049] If the **likelihood of an attack succeeding** can be estimated for a number of different threats, then this can be combined with knowledge of the logical structure of IT systems 30 (FIG. 3) within the network 1 and knowledge of processes 31 (FIG. 3) dependent on those IT systems 30 (FIG. 3) **to predict, for a given period of time, loss to the organization due to these threats**. In some embodiments, the **predicted loss** is expressed as a value at risk (VAR). However, **the prediction** may be expressed as any value or figure of merit which characterises or quantifies loss to the organisation arising from operational processes being disabled.

(emphasis added). More to that point, paragraph [0061] states that

> The severity score ("SeverityScore") is a measure of the impact of a successful threat. It is **not** a measure of the prevalence or exposure to the threat, but rather an indication of the damage **that would be caused** to the target system.

Accordingly, the application as originally filed adequately supports amending independent claims 1, 27, and 31, to specify that the threat being predicted is "future" threat, and as such are distinguished from Gong.

Regarding the amendments to the independent claims that the stochastic modeling is of "past observed" threat events, support for those amendments is also found throughout the application as originally filed. For example, paragraphs [0054] through [0057] disclose:

> [0054] A module 6 (hereinafter referred to as a "threat analyser") **samples incoming traffic 4 and identifies threats using a list 7 of known threats stored in a database 8**. For example, the module 6 may be a computer system running SNORT (for example release 2.6.0.1) available from www.snort.org.
>
> [0055] The threat analyser 6 produces **observed threat data** 9, which includes **a list of observed threats** and their frequency of occurrence, and stores the data 9 in a database 10. [0056] In some embodiments of the present invention, a system 11 for assessing threat uses models threats to the corporate network 1 so as **to predict loss** 12 **arising from these threats** and/or to provide feedback 13 to the firewall 3.

> [0057] Each **observed threat** is defined using an identifier, a name, a description of the threat, a temporal profile specify-ing frequency of occurrence of the threat, a target (or targets) for the threat and a severity score for the (or each) target.

(emphasis added). As demonstrated, unambiguous basis can be found throughout the specification for the amendments made to independent claims 1, 27, and 31, concerning "past observed" threat events, and accordingly further distinguishes the subject matter claimed therein from Gong.

The amendments presented above sufficiently distinguish the independent claims from Gong, which is directed to continued operation during an on-going intrusion. This is readily apparent from, e.g., the summary of the invention, which states:

> The present invention relates to an intrusion tolerant server system that includes a network interposed between a client and a protected server. **It minimizes the impact of intrusive events and permits continued operation in the face of intrusion attacks.**

(emphasis added); *see also*, paragraph [0014] (confirming the invention concerns "detecting [actual] threats" and reconfiguring components in response thereto"). Gong does not concern predicting future threats using past observed threat events as the present application does, but rather, Gong is directed to detecting a current intrusion, minimizing the occurring damage, while maintaining operation of a server during the intrusive event. Specifically, paragraphs [0054] through [0055] of Gong state:

> [0054] Operating in the low overhead configuration still requires vigilance by the intrusion sensor 50 and adaptive reconfigurer 60. **Upon detection of an intrusion event,** the adaptive reconfigurer **alters** the tolerance protocol **and reconfigures** the network forwarding scheme **to distribute the functions** of the acceptance monitors, ballot monitors and proxy servers **to provide the requisite redundancy or isolation to minimize the impact** of such a threat, including reconfiguration as shown in FIG. 2.
>
> [0055] One consideration regarding strategies for intrusion tolerance is to **determine,** as best possible**, the actual level of security threat**. This **threat level directly impacts the level of redundancy required to ensure dependable service** and

> maintain desired efficiencies. The highest level of threat protection, as illustrated in FIG. 2, provides redundant servers, balloters and acceptors; each assigned to a given request in parallel. Different levels of service are available, as distinguished in Type 1 and Type 2 service in FIG. 2. At the other end of the spectrum, **zero redundancy is appropriate if there is no threat.** An intermediate strategy may designate redundant servers as primary, secondary, tertiary, backup, etc. The primary server S is invoked first to process a request and additional servers are invoked for a given request only when necessary. **In the absence of intrusions or faults, backup servers may be released for other tasks.**

(emphasis added). As disclosed, Gong concerns detecting a current intrusion, determining an actual level of threat of the current intrusion, handling that current intrusion, minimizing the damage occurring because of the current intrusion, and keeping servers operational during the current intrusion, such that when no intrusion is detected server redundancy is not needed to otherwise ensure dependable operation. Accordingly, Gong is concerned with handling and analyzing current intrusions and the actual threat level of those current intrusions, and is not concerned with analyzing past observed threat events in order to predict future threats.

Thus, the disclosure of Gong is directed to current intrusions and specifically states that when no intrusion is currently detected the measures otherwise taken to ensure operation of the servers are not needed. As such, Gong does not disclose every element of currently amended independent claim 1, 27, or 31, because Gong does not describe predicting future threat activity based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate.

Therefore, currently amended independent claims 1, 27, and 31, and all claims 2-26, 28-30, and 33-34, depending therefrom, are novel and non-obvious over Gong. Applicant respectfully requests withdrawal of the rejections of the independent claims, as well as all claims depending therefrom.

Rejections under § 103(a)

Each of the dependent claims stands rejected over Gong in view of other references. Specifically, claims 4 and 5 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gong in view of U.S. Patent Application Publication 2009/0204471 to Elenbaas. Claims 6-15 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gong, and Elenbaas, in further view of U.S. Patent Publication No. 7,409,716 to Barnett. Claims 16-23, 25, and 26, are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gong, Elenbaas, Barnett, and in further view of U.S. Patent Application Publication No. 2005/0066195 to Jones. Applicant respectfully traverses these rejections. In short, none of the cited art cures the deficiencies of Gong or would render the claims obvious.

Dependent Claim 26

Concerning claim 26, which stands rejected under 35 U.S.C. § 103(a), the Office Action alleges that Gong, Elenbaas, and Barnett, in further view of Jones, set forth all elements of the claim, and alleges that a sufficient motivation existed at the time of the invention for modifying the combination of Gong, Elenbaas, and Barnett with the subject matter of Jones such that a person having ordinary skill in the art would have arrived at the invention as recited in claim 26. Specifically, the Office Action relies on paragraph [0184] of Jones, which states:

> Responsive controls mechanisms and processes have three primary purposes: **To contain** the effect a threat agent **is having** on an object, **to investigate and remediate** (if possible) the source of the threat, and **to recover** the information or systems affected by the event.

(emphasis added). In short, Jones (like Gong) relates to a current, on-going threat and not a predicted, future threat, as claimed. Therefore, the recited functions do not correspond to the functions of the specified first and second modules, namely: "*a first module configured to predict future threat activity and to output the predicted future threat activity to a second module*" wherein such future threat activity is predicted "*based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate*." Neither Gong nor, Elenbaas, nor Barnett, nor Jones, concern the elements of

predicting future threat using past observed threat events, and the content of Jones, as emphasized above, is clearly directed to current threat analysis, remediation, and recovery.

Claims 33 and 34 include similar limitations. Therefore, dependent claim 26, as well as claims 33 and 34, are neither anticipated nor rendered obvious by Gong, Elenbaas, Barnett, or Jones, whether considered alone or in combination. Based on the foregoing, withdrawal of the rejection of claim 26 under 35 U.S.C. § 103(a) is respectfully requested.

CONCLUSION

In view of the foregoing it is believed the application is in condition for allowance and it is respectfully requested and that all pending claims be allowed and the case passed to issue.

This response is being filed with a request for three-month extension of time, the fee for which is enclosed herewith. If any additional fees are due, the Commissioner is hereby authorized to charge any unpaid fees deemed required in connection with this submission, including any additional filing or application processing fees required under 37 C.F.R. § 1.16 or 1.17, or to credit any overpayment, to Deposit Account No. 19-4709.

In the event that there are any questions, or should additional information be required, or if examination can be expedited through clarification or discussion, the Examiner is invited to contact Applicant's attorney at the number listed below.

Respectfully submitted,

/Ian G. DiBernardo/

Ian G. DiBernardo
Reg. No. 40,991
Attorney for Applicant
Stroock and Stroock and Lavan LLP
180 Maiden Lane
New York, New York 10038
(212) 806-5400