US008898784B1

(12) **United States Patent**
Alexander et al.

(10) **Patent No.: US 8,898,784 B1**
(45) **Date of Patent: Nov. 25, 2014**

(54) **DEVICE FOR AND METHOD OF COMPUTER INTRUSION ANTICIPATION, DETECTION, AND REMEDIATION**

(71) Applicants: **Keith B. Alexander**, Ft. Meade, MD (US); **Patrick W. Dowd**, Annapolis, MD (US); **Robert L. Grossman**, River Forest, IL (US)

(72) Inventors: **Keith B. Alexander**, Ft. Meade, MD (US); **Patrick W. Dowd**, Annapolis, MD (US); **Robert L. Grossman**, River Forest, IL (US)

(73) Assignee: **The United States of America, as represented by the Director, National Security Agency**, Washington, DC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/573,931**

(22) Filed: **May 29, 2013**

(51) **Int. Cl.**
G06F 12/14 (2006.01)
G06F 15/16 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/145*** (2013.01)
USPC **726/23**; 709/232

(58) **Field of Classification Search**
CPC H04L 63/14; H04L 63/16; H04L 63/20; H04L 63/1433; H04L 12/56; G06F 15/173
USPC 726/2, 23, 25, 26, 24, 27; 713/13, 15, 713/23; 709/232, 228, 238; 370/401, 229, 370/218
See application file for complete search history.

(56) **References Cited**

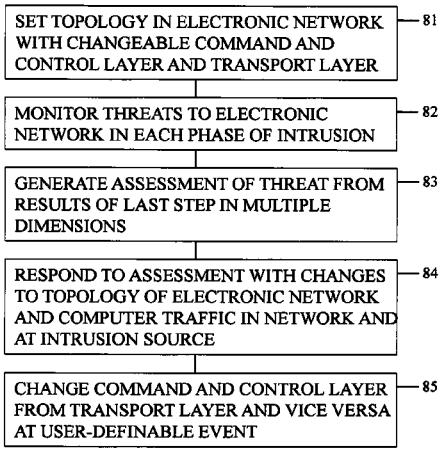
U.S. PATENT DOCUMENTS

5,966,531 A * 10/1999 Skeen et al. 719/315
6,564,258 B1 * 5/2003 Uniacke 709/223
6,839,003 B2 * 1/2005 Soliman et al. 341/50
7,263,290 B2 * 8/2007 Fortin et al. 398/58
7,506,050 B2 * 3/2009 Glasmann et al. 709/224
7,665,097 B2 2/2010 Rodrigues et al.
7,697,420 B1 * 4/2010 Garahi et al. 370/229
7,895,452 B2 * 2/2011 Mir et al. 713/193
8,112,642 B2 * 2/2012 Bose et al. 713/300
8,261,355 B2 9/2012 Rayes et al.
2003/0182437 A1 * 9/2003 Kobayashi et al. 709/232
2004/0027259 A1 * 2/2004 Soliman et al. 341/50
2004/0128397 A1 * 7/2004 Glasmann et al. 709/232
2004/0264371 A1 * 12/2004 Chen 370/229
2005/0213608 A1 * 9/2005 Modi et al. 370/468
2006/0101511 A1 * 5/2006 Faillenot et al. 726/13
2007/0064617 A1 * 3/2007 Reves 370/252
2007/0198863 A1 * 8/2007 Bose et al. 713/300
2007/0253341 A1 * 11/2007 Atkinson et al. 370/252
2008/0196104 A1 * 8/2008 Tuvell et al. 726/24
2009/0049318 A1 * 2/2009 Bose et al. 713/320
2009/0067440 A1 * 3/2009 Chadda et al. 370/401
2010/0138097 A1 * 6/2010 Ku et al. 701/27
2010/0205315 A1 * 8/2010 Xia 709/228
2011/0103394 A1 5/2011 Vogt et al.
2011/0119390 A1 5/2011 Leech et al.

(Continued)

Primary Examiner — Abu Sholeman

(57) **ABSTRACT**

Electronic network security by establishing a network topology, including multiple devices, where the network includes a command and control layer and a transport layer, where the command and control layer is changeable by the transport layer and vice versa. All phases of an intrusion attempt are monitored to anticipate an intrusion, prevent an intrusion, and remedy a successful intrusion. An assessment of the threat is made in multiple dimensions. The topology of the network may be changed in accordance with the threat assessment. In addition, computer traffic in the network and from the intrusion source may be modified or stopped to guard against an intrusion, prevent an intrusion, and remedy a successful intrusion. The command and control layer is changeable by the transport layer and vice versa.

12 Claims, 5 Drawing Sheets