NetNumber Delivers First Multi-Protocol Signaling Firewall for Telecom Networks

NetNumber TITAN Expands SS7 Security Protection to Include All Signaling Protocols for Next-Gen and IoT Networks

LOWELL, Mass. and Barcelona, Spain — February 23, 2016 — NetNumber announced today the industry's most comprehensive multi-protocol signaling firewall on its TITAN Centralized Signaling and Routing Control (CSRC) platform. Building on last year's delivery of the NetNumber SS7 Firewall application, NetNumber is now providing the same level of firewall capabilities for all signaling protocols including the addition of Diameter, SIP, HTTP and DNS/ENUM. As these firewall applications can be combined seamlessly with other NetNumber applications such as an STP, DSC, HSS or HLR on the same TITAN platform, telecom operators have an unprecedented level of multi-protocol signaling protection, flexibility and operational uniformity in a platform that can reduce Opex/Capex costs and improve efficiency.

The security of the signaling network is at risk today due to several factors, including new telecom operators requiring mobile roaming interconnection and the use of femtocells with direct signaling access. With up to 20-30 billion network connected devices, applications and sensors predicted by 2020, the Internet of Things (IoT) represents a critical challenge for operators in terms of signaling and security. The very high level of authentication and registration events, signaling traffic bursts, unpredictable effects of these unmanaged devices, complex network interconnection scenarios, and possible hostile hacker attacks all pose real threats to networks supporting IoT traffic. Telecom operators need a new, highly secure signaling architecture protected by a robust multi-protocol signaling firewall as delivered in NetNumber TITAN to address these challenges.

According to Deborah Kish, principal research analyst, and Lawrence Pingree, research director, at Gartner, "Wireless CSPs rolling out voice over LTE (VoLTE) and LTE-A will need to put in place components and configurations to ensure quality of service, prevent legitimate network failures and fend off malicious attacks. In addition, with VoLTE maturing, protecting and

controlling session initiation protocol (SIP) and the IP Multimedia Subsystem (IMS) architecture will be a focus for CSPs. VoLTE and IMS are based on the SIP protocol and security of the protocol. The IMS architecture is that which is responsible for the setup and teardown of sessions, as well as where the home subscriber server (HSS) may reside. Compromising the HSS would give hackers access to subscriber data and services, and therefore, it must be protected." (Gartner, Competitive Landscape: Carrier-Class Network Firewalls, November 15, 2015)

"The security issues with SS7 networks have been top of mind for telecom operators lately as researchers and operators alike have shared threat and vulnerability details," said Matt Rosenberg, vice president of NetNumber Global Sales, Solution Design, and Product Management. "We are seeing similar concerns with other existing and new signaling protocols such as Diameter as mobile roaming access and IoT device deployment increase. Signaling firewalls are quickly becoming critical to protecting the telecom operator networks. As these networks deploy a variety of signaling protocols, NetNumber has responded by delivering the industry's most comprehensive multi-protocol signaling firewall application in the TITAN CSRC platform for unprecedented protection."

NetNumber is an associate member of the GSMA, and with its active participation in the Fraud and Security Group (FASG), NetNumber is working to ensure the TITAN SS7 Signaling Firewall protects against all SS7 Category 1, 2, and 3 threats. This equally applies to the Diameter and other signaling protocol vulnerabilities as well as vulnerabilities that may encompass a combination of signaling protocols.

A comprehensive monitoring function completes the NetNumber Multi-Protocol Signaling Firewall to offload data to external systems for big data analytics, reporting, statistics and other auxiliary functions used by telecom operators to build a complete next-generation signaling protection capabilities in today's complex and geo-dispersed networks.

TITAN provides a common, virtualized infrastructure for all signaling control, routing policy enforcement and subscriber database services in the network. It uniquely delivers centralized provisioning and management combined with a powerful distributed, in-memory database replication method that enables all signal processing to happen at the optimal location in an operator's network. TITAN is transforming how operators deliver new services to their customers while significantly simplifying the network core and reducing operating costs. Today,

TITAN is deployed on more than 350 servers on five continents, and supports more than 200 billion transactions per month.

Learn more about TITAN at http://netnumber.com/products/titan/ or by contacting sales@netnumber.com.

About NetNumber

NetNumber, Inc. brings 15 years of experience delivering innovative signaling control solutions that enable carriers to accelerate implementation of new services across multiple generations of networks, while dramatically simplifying the core network and reducing operating costs. Today, we are the leading provider of Centralized Signaling and Routing Control (CSRC) solutions to the global communications industry. Visit www.netnumber.com for more information. Connect with us on Twitter, LinkedIn, Google+ and Facebook.

# # #

Contact Information:
Kim Gibbons
+1 408 398 5223
kgibbons@netnumber.com