NetNumber Locks Down End User Credentials on Mobile Access Networks

Delivers Ut Proxy Application on TITAN Platform for Mobile Operators

LOWELL, Mass. — Dec. 17, 2015 — NetNumber today announced availability of the Ut Proxy application on the industry's most robust centralized signaling and routing (CSRC) platform, TITAN. With the new wave of IMS services such as VoLTE, VoWiFi and RCS, mobile operators are opening their IMS application domains via a variety of access networks like LTE, non-3GPP (WiFi) and DSL. This introduces security challenges as the IMS application domain is not protected by the authentication procedures applied during access. An additional network element, Ut Proxy, must be introduced to protect the IMS application domain from being directly accessed by the end user device—and possibly inserting security vulnerabilities. Authentication and access authorization procedures must be implemented for the HTTP transport protocol.

"Signaling layer vulnerabilities are an issue for all service providers," said Patrick Donegan, chief analyst, Heavy Reading. "Whether it be legacy protocols like SS7, or newer IP protocols, signaling threats have the potential to cause data leakage and network disruption and need to be addressed."

The NetNumber Ut Proxy application provides HTTP access to 3GPP authentication mechanisms for devices with and without SIM cards. Leveraging the NetNumber TITAN CSRC model, the Ut Proxy application can be combined on the same centralized platform with other functions like HLR, HSS, AuC, AAA and DSC via service chaining. Mobile operators now have a robust and flexible solution for establishing a secure end-to-end connection between a customer's mobile device and the IMS service domain using different technologies —without exposing end user credentials and without the need for provisioning additional credentials.

"Increasingly, mobile operators are concerned with security," said Matt Rosenberg, vice president of NetNumber Global Sales, Solution Design and Product Management. "Security threats and breaches put customer data at risk and impact quality of service. The transition to next-generation networks further complicates security and exposes threats. NetNumber is focused on

addressing these most pressing security challenges with a comprehensive suite of security applications in TITAN that interwork and support the transition from legacy to next-generation networks."

NetNumber TITAN is transforming how operators deliver new services to their customers while significantly simplifying the network core and reducing operating costs. TITAN provides a common, virtualized infrastructure for all signaling control, routing policy enforcement and subscriber database services in the network. Only NetNumber can deliver SS7/C7, SIGTRAN, ENUM, DNS, SIP, HTTP, RADIUS and DIAMETER services on the same signaling-control platform while centralizing the provisioning and simplifying the network's OSS/BSS layers.

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