Mobile versus Mobile: 867-5309

Lori MacVittie, 2012-12-03

#mobile #context *The identity crisis created by common platforms negatively impacts the ability to serve consumers and corporate IT consistently*

The focus on the explosion of mobile devices is heavily weighted toward IT in terms of management and security. While there's nothing wrong with it, there's another aspect of mobility that is often ignored. Much like their tethered counterparts, many mobile devices are constrained by a tight-coupling to numbers. In the case of the desktop it's often IP address. In the mobile word, it's another number: your phone number.

I love my tablet, I really do. And I love mobile applications. But what I don't love is mobile applications that, while perfectly able to run on my tablet and written for the same OS that powers many smart phone mobile devices, require tethering to a phone number.

Because, Hello? McFly!?! It doesn't have a phone number!

NUMBER-BASED IDENTITY

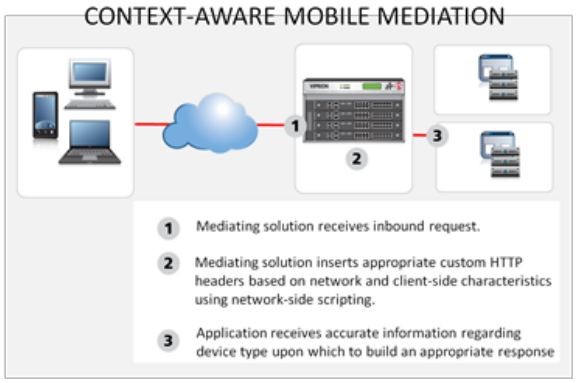
We're going to skip the Prisoner analogy and just assume it was made, okay? While it's always applicable to discussions this, it gets a bit tedious and cliché after a while and so let's just assume that tethering identity to a number of ***any*** kind is a Very Bad Idea™, m'kay? In the tethered world this is because such numbers are – especially today – highly volatile. You can't count on even an application instance having the same IP address from one minute to the next let alone a user who may be roaming around the world. And in the mobile world, it's even less of a sure bet as mobile devices of all kinds are moving between WiFi and mobile network faster than a four-year old tears open a Christmas present.

We (as in IT) simply cannot enforce corporate security and serve the access needs of a highly nomadic user community if we're constrained to doing so based on a single number – whether it be IP address or phone number. We've got to leverage as much information as possible about the user – their network, the device, their location, the security posture of the end-point. We've got to take into consider the context of each and every request and use that data as the basis for allowing or denying (or at least limiting) access to corporate resources.

Mobile applications requiring phone-number do so as a means to secure access to resources. It is a failure of Epic Proportions because it tends to engender a false sense of security on the IT side, based on the premise that phone number is unique to an individual and highly static, which is not always the case. It is a failure of Epic Proportions because it stratifies a much larger technological market into "haves" and "have nots" based on whether a single identifying characteristic is present: a number.

Such strategies are further a Very Bad Idea™ because of the impact on policy management and security and development. Applications relying on numbers for identity work only on devices that have such numbers; for the rest of the market (which is growing by leaps and bounds as more and more consumer devices are Internet-enabled) there must exist a separate but equal application. Developers time is already strapped, and maintaining two (in some cases three when the web is considered separately from mobile devices) discrete applications is madness, I say, madness. The pressure on IT to secure, manage, and support multiple versions of the same application were supposed to go the way of the Dodo with the advent of REST and the ascendancy of the API.

And yet here were are, managing and securing and developing applications tied to numbers.



MOBILE-MEDIATION

You may recognize this one from a previous post, "Mobile versus Mobile: An Identity Crisis", and it's no less applicable to this problem than it was to the problem of mobile clients and OS or platform-based identification. Whether it's OS, platform, or IP address/phone number, no single characteristic of a user's request is enough information upon which to base any kind of decision.

Period.

No single piece of information gives IT the context in which security and delivery decisions can be accurately made. Without the big picture, without the ***context,*** it is nigh-unto impossible to ascertain which decision should be made with respect to the request. It is only by taking advantage of context that we can make decisions that are not only best for the organization and preserve a positive security posture, but that are also best for the user in terms of experience and performance.

It is only at strategic points of control in the network, such as the application delivery tier, that all the variables on both sides of the equation – user and data center – are visible. It is at this tier where the rubber meets the road, as they say, and the two worlds of consumer and corporate meet. It is here where security and performance and access policies are most efficiently applied, where all the requisite variables that make up the ***context*** of the request can be extracted, evaluated, and acted upon.

It is paramount to both end-user adoption and a positive corporate operational posture that such strategic points of control are leveraged. It is only context that provides insight into the "bigger picture" and ensures a smooth and secure experience for end-users that simultaneously preserves the security and availability of the applications and resources being delivered.

Mobile users are not a number, nor are their tethered counterparts. They are users, with unique characteristics that are increasingly not only varied but volatile. Such variables must be evaluated contextually for every request to ensure the best possible experience without compromising operational or business expectations and requirements.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com