



**The George Washington University  
Department of Computer Science  
Colloquium**

**February 25, 2008, 11:00am  
Room 736 Academic Center**

**Apu Kapadia  
Dartmouth College**

**Accountable Anonymity**

**ABSTRACT**

Anonymizing networks such as Tor allow users to access Internet services privately using a series of routers to hide the client's IP address from the server. Tor's success, however, has been limited by users employing this anonymity for abusive purposes, such as defacing Wikipedia. Website administrators rely on IP-address blocking for disabling access to misbehaving users, but this method is not practical if the abuser routes through Tor. As a result, administrators block all Tor exit nodes, denying anonymous access to honest and dishonest users alike. A few bad apples spoil the fun for everybody. To address this problem, the author presents a low-overhead credential system called Nymble to provide "anonymous blacklisting." With Nymble, (1) honest users remain anonymous; (2) a server can complain and blacklist an anonymous user to recognize future connections from that user; and (3) users are aware of their blacklist status and can thus choose to remain anonymous by not accessing the service. As a result of these properties, the author's system is agnostic to servers' varying definitions of misbehavior – servers can blacklist any user, for whatever reason, and users need not worry about a reduction in privacy from such blacklisting.

**BIOGRAPHY**

**Apu Kapadia** received his Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign (UIUC) in October 2005. For his dissertation research on trustworthy communication, he received a four-year High-Performance Computer Science Fellowship from the Department of Energy. Following his doctorate, he joined Dartmouth College as a Post-Doctoral Research Fellow with the Institute for Security Technology Studies (ISTS). He is interested in topics related to systems security and privacy. He is particularly interested in accountable anonymity, privacy-enhancing technologies such as anonymizing networks, usable models and policy languages for privacy, and applied cryptography.