



# IEEE Okanagan Subsection Presents

**Dr. William J. Blanke**  
Nok Nok Labs, Palo Alto, CA USA



## **iOS Interprocess Communication Security and the Universal Authentication Framework Protocol**

**Time & Date:** 5 pm – 6 pm, May 26th, 2015.

**Location:** E103, [Okanagan College](#), 1000 KLO Rd, Kelowna, BC V1Y4X8 ([parking info](#)).

**Talk Abstract:** The Universal Authentication Framework (UAF) protocol is a newly ratified, public key cryptography-based standard from the FIDO Alliance that supplants the common shared-secret login password. To achieve this, a UAF client on a user's device mints public key pairs on a per-relying party basis, and registers the public key with the relying party server. The UAF client then manages the private keys, which are used to sign server-generated authentication challenges. The prior-registered server-side public keys are then used to verify the signed challenge responses in order to authenticate the user session.

On the iOS platform, the UAF client can exist as a standalone app that services authentication requests from other apps (termed relying party apps in UAF parlance) via custom URL schemes for interprocess communication. This presentation first will identify the strengths of using custom URL schemes for communication between relying party apps and a standalone UAF client. Second, the presentation will analyze the threats to this approach and will illustrate their mitigation by the UAF standard.

**Speaker Biography:** I graduated with my BSE from Duke University (2015 NCAA champs! Go Blue Devils!), MS from the University of Virginia, and PhD from the University of Texas at Austin. I specialize in security software for Windows, iOS, and Android. Currently as the mobile lead architect at Nok Nok Labs, a Silicon Valley startup, I helped create the first FIDO enabled multifactor authentication client for Android and iOS. If you own a Samsung Galaxy S5, you might already be using our software! My security focus results from a decade as a technical director at PGP Corporation (a division at Symantec), where I developed the PGP product line for Windows, Windows CE, Windows Mobile, and iOS. Previously, I taught graduate and undergraduate courses as a lecturer of Computer Science at the University of the South Pacific, in Suva, Fiji Islands.

**Refreshments** will be provided. For further information please contact:

Youry Khmelevsky (email: [youry@ieee.org](mailto:youry@ieee.org)). Registration Page:

<https://meetings.vtools.ieee.org/m/34489>