

TRACK: IT Security Advanced
SESSION #: ITA#9
DATE: Tuesday April 20, 2010
TIME: 2:55-4:10pm
SESSION TITLE: "Leveraging Network Configuration Change Management for Network Attack Investigation"
SPEAKER(S): Alan M. Carroll, Ph.D. – CEO and Founder
ORGANIZATION: Network Geographics, Inc.

ABSTRACT: "Leveraging Network Configuration Change Management for Network Attack Investigation"

Most organizations employ some degree of change management over their network device configurations. At a minimum this involves an approval process but should and generally does include maintaining a historical record of configurations for each device by hand or (preferably) with a source control system.

By using change management for network configurations, the organization improves reliability and dependability of their network infrastructure. In addition, change management gives an organization a number of options for network debugging and forensics. In this talk we will describe procedures for conducting a forensic search on configurations in the case of a security event. We will work through a running example to illustrate how a security investigator can leverage an archive of network configuration files. With good records such techniques can locate the time of and responsibility for the configuration changes that permitted the security event.

We will demonstrate how new technologies in configuration modeling make this far more feasible than has been the case when such a search would have to be conducted manually through visual inspection of configurations or network probing alone.

Beyond locating the root cause of a problem, change management provides a framework for the introduction of preventative security/error checks. We will discuss techniques to automate as much of the process as possible. The end goal is to "close the loop" and create IT staff and a set of procedures that can continuously improve to cope with the ever increasing demands by learning from the past as well as looking to the future.

SPEAKER BIO(S): Dr. Alan M. Carroll is the CEO and founder of Network Geographics. At Network Geographics he leads development of innovative products in the area of network security management and maintenance.

He has consulted in the area of policy-based security management, software forensics, and general system design. In his spare time, Dr. Carroll is interested in web-based software. He is the author of the widely used MTAutoban plugin for the Moveable Type platform.

Dr. Carroll earned a PhD from the University of Illinois, while building Epoch, the first windowed version of Emacs, and ConversationBuilder, a collaborative development environment. He worked for a series of startups ending at Global Internet Software Group on a team developing Centri Firewall for Windows NT. Global Internet Software Group was acquired by Cisco Systems. At Cisco Systems, Alan led infrastructure development efforts in network security and policy management software.