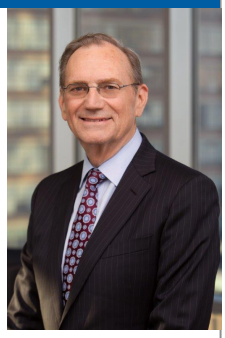
Mark Graff

Founder & CEO
TellAGraff, LLC



A cyber security practitioner and thinker for almost 30 years, Mark Graff is the Founder & CEO of TellAGraff, LLC.

He is also the founding chair of the Cyber Security Working Group of the World Federation of Exchanges, the first-ever forum for communication amongst information security heads of the world's exchanges. Most recently, Graff has served as the head of cyber security for NASDAQ, as the Chief Information Security Officer.

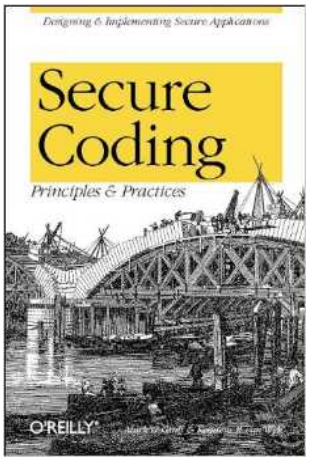
Formerly Chief Cyber Security Strategist at Lawrence Livermore National Laboratory, he has appeared as an expert witness on computer security before both Congress and the Presidential Commission on Infrastructure Survivability, and served as an expert witness on electronic voting machine software for the state of California.

A past chairman of the international Forum of Incident Response and Security Teams (FIRST), Graff has lectured on risk analysis, the future of cyber security and privacy, and other topics before the American Academy for the Advancement of Science, the Federal Communications Commission, the Pentagon, and many other U.S. national security facilities and "think tanks."

Table of Contents

2 Books by Mark Graff

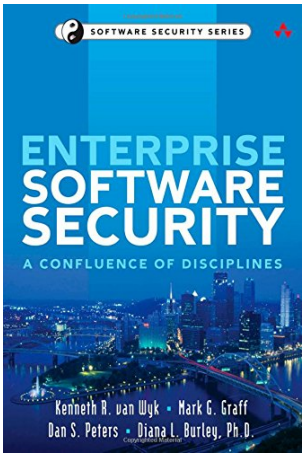
3 News Articles



Secure Coding
Principles & Practices

Secure Coding, by Mark Graff and Ken vanWyk, has been used at dozens of universities around the world to teach how to design and build secure software-based systems. *Secure Coding* looks at the problem of bad code in a new way. Packed with advice based on the authors' decades of experience in the computer security field, this concise and highly readable book explains why so much code today is filled with vulnerabilities, and tells readers what they must do to avoid writing code that can be exploited by attackers. Writing secure code isn't easy, and there are no quick fixes to bad code.

Beyond the technical, *Secure Coding* sheds new light on the economic, psychological, and sheer practical reasons why security vulnerabilities are so ubiquitous today. It presents a new way of thinking about these vulnerabilities and ways that developers can compensate for the factors that have produced such unsecured software in the past. It issues a challenge to all those concerned about computer security to finally make a commitment to building code the right way.



Enterprise Software Security:
A Confluence of Disciplines
(Addison-Wesley Software Security Series)

Traditional approaches to securing software are inadequate. The solution: Bring software engineering and network security teams together in a new, holistic approach to protecting the entire enterprise. In *Enterprise Software Security*, Mark Graff, Kenneth vanWyk, Dan Peters, and Diane Burley, Ph.D. explain why this “confluence” is so crucial, and show how to implement it in your organization.

Writing for all software and security practitioners and leaders, they show how software can play a vital, active role in protecting an organization. Readers learn how to construct software that actively safeguards sensitive data and business processes and contributes to intrusion detection/response in sophisticated new ways. The authors cover the entire development lifecycle, including project inception, design, implementation, testing, deployment, operation, and maintenance. They also provide a full chapter of advice specifically for Chief Information Security Officers and other enterprise security executives.

Enterprise Software Security delivers indispensable big-picture guidance– and specific, high-value recommendations readers can apply right now.

News Articles

Global Stock Exchanges Band Together on Cybersecurity Initiative

"A worldwide group of top stock exchanges have gotten together to launch the industry's first cybersecurity committee, with a mission to aid in the protection of global capital markets."

Full Article:
http://www.infosecurity-magazine.com/view/36234/global-stock-exchanges-band-together-on-cybersecurity-initiative/

Three Tactics for Cyberdefense

"Filtering network traffic and educating employees are among the steps companies can take steps to harden their attack profile and increase chances of detecting or deflecting an Advance Persistent Threat-style attack"

Full Article:
http://blogs.wsj.com/cio/2013/04/04/three-tactics-for-cyberdefense/

How Exchanges Should Tackle Cybersecurity

"The financial services sector is at the forefront of proactive cybersecurity. Crucial to the success of finance is the need to reach across competitive aisles and geographic borders to share best practices and protect customers from cyberattacks."

Full article:
http://www.institutionalinvestor.com/blogarticle/3325606/Blog/How-Exchanges-Should-Tackle-Cybersecurity.html?ArticleID=3325606&eventlogin=Login&login=1&actionname=login&eid=E017#.U16M1ZG4nHg

Sidebar: More Tips for Preventing Insider Abuse

"A variety of expert tips on preventing security breaches by employees."

Full Article:
http://www.computerworld.com/s/article/82930/Sidebar_More_Tips_for_Preventing_Insider_Abuse

For more information, contact Sahl Communications:
1 West Broad Street, Suite 904, Bethlehem, PA 18015
484.892.9926
SahlComm
SAHL COMMUNICATIONS, INC.