



American Society for Quality (ASQ) — Washington, DC & Maryland Metro Section (509), Software Special Interest Group (SSIG)
IEEE Computer Society — Washington, DC & Northern Virginia Chapters
Society for Software Quality (SSQ) — Washington, DC Area Chapter

Understanding How the Bad Guys Attack Your Software: CAPEC

by: Sean Barnum

Tuesday February 21, 2012

Security is quickly becoming a primary concern in the development of software today and security knowledge will increasingly become a required arrow in the software developer's quiver. By learning to think more like attackers, we gain a better understanding of how to defeat their methods. The Common Attack Pattern Enumeration and Classification (CAPEC™) initiative is a community-driven software security effort to create a publicly available catalog of attack patterns. At the core of CAPEC is the concept of an "Attack Pattern," a powerful mechanism for capturing and codifying various approaches to cyber attack, including the detailed action-oriented attack execution flow, the capability and motivation of the attacker, the context within which the attack is possible, the weaknesses being targeted by the attack, characterization of the typical impact of a successful attack, and recommended mitigations to prevent or decrease the impact of the attack. This talk will serve as an overview of the CAPEC project to-date and discuss some of the various uses cases for CAPEC in software development, testing, architecture analysis, and secure operations.

Sean Barnum is a Cyber Security Principal at The MITRE Corporation where he acts as a thought



leader and senior advisor on software assurance and cyber security topics to a wide variety of US government sponsors throughout the national security, intelligence community and civil domains. He has over 25 years of experience in the software industry in the areas of architecture, development, software quality assurance, quality management, process architecture & improvement, knowledge management and security. He is a frequent contributor, speaker and trainer for regional, national and international cyber security and software quality publications, conferences, and events. He is very active in the Cyber Security community and is involved in numerous knowledge standards-defining efforts including the Common Weakness Enumeration (CWE), CAPEC, the Software Assurance Findings Expression

Schema (SAFES), the Malware Attribute Enumeration and Characterization (MAEC), the Cyber Observables eXpression (CyBOX) and other elements of the Cyber Security Programs of the Department of Homeland Security, Department of Defense, and NIST. He is coauthor of the book "Software Security Engineering: A Guide for Project Managers", published by Addison-Wesley. He serves as the official liaison between ISO/IEC JTC 1/SC 27/WG 3 and the Cyber-Security Naming & Information Structures Group. He also acted as the lead technical subject matter expert for design and implementation of the Air Force Application Software Assurance Center of Excellence (ASACoE).

Tuesday February 21, 2012

5:30 PM – Networking and Pizza(*)

5:50 – 6:50 PM – Program

(*) *There is no cost to attend at McLean and Silver Spring.*

Locations:

The presentation will originate at the McLean facility, with video tele-conferencing (VTC) between:

MITRE-2, room **1N100**
7515 Colshire Drive
McLean, VA 22102
host: Scott Ankrum
cell: 240-731-7581

FDA, Bld 66, room **G512**
10903 New Hampshire Ave
Silver Spring, MD 20993
host: James Simpson
cell: 301-996-4976

Your location
could be here!

MITRE, room **1M306**
202 Burlington Rd (Rt. 62)
Bedford, MA 01730
host: Tim Rice
cell: 978-758-2704

If you can host another location via VTC, please contact Scott Ankrum (below)

TO ATTEND THE MeetingPlace Collaboration CONFERENCE:

1. Go to: <http://audioconference.mitre.org/> 2. Click on Attend Meeting. If MeetingPlace Collaboration Window does not automatically open, press connect. 3. Dial your telephone to connect to the audio of the meeting.

- Dial 703-983-6338 (x36338) from the Washington DC region.
- Dial 781-271-6338 (x16338) from the Bedford, MA region.

Meeting ID: 509509, when prompted. Meeting Password: 05090509, when prompted.

Visit <http://audioconference.mitre.org> to test your web browser for compatibility with the web conference. Follow this link to the browser test link on the page.

Registration:

Registration Website: <http://www.asq509.org/ht/d/DoSurvey/i/26913>

You must register by noon on Monday, February 20. If you cannot attend at any location, select telephone dial-in when you register. To RSVP for FDA (Silver Spring), please indicate citizenship. If not a US citizen, please provide your title, employer, and address. Allow 2 business days for registration before the meeting.

For registration problems or further information contact Scott Ankrum at: ankrums@mitre.org or 703-983-6127

Software SIG Chairman: T. Scott Ankrum (ASQ & IEEE)

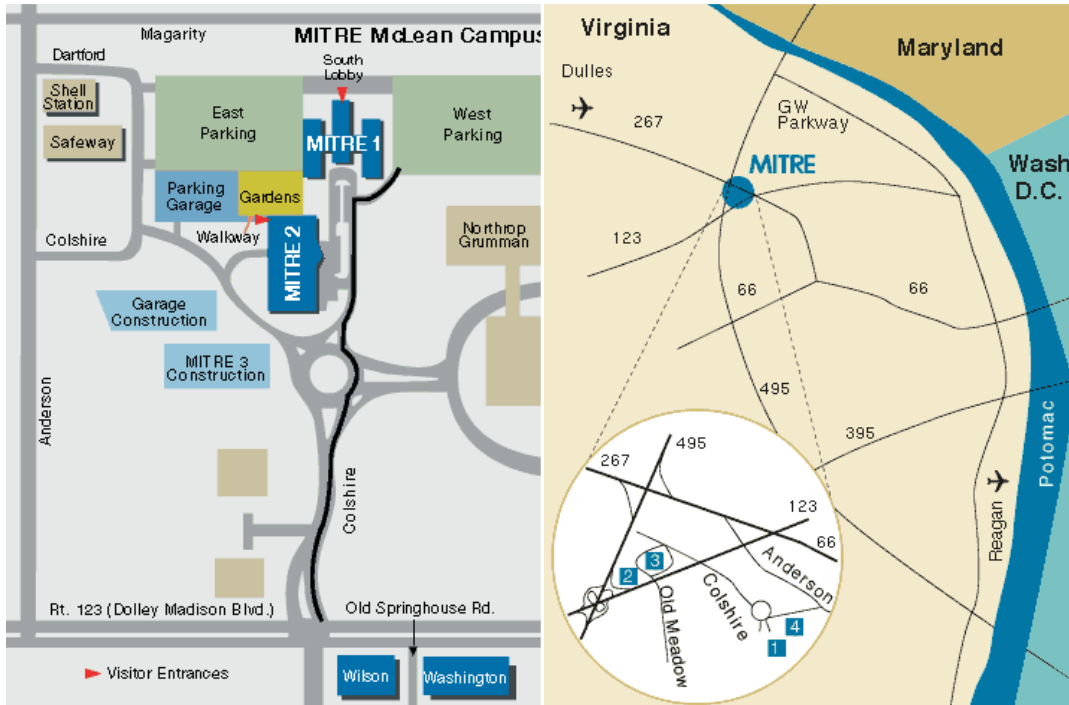
Software SIG Committee: Richard Eng (ASQ); Chris Jones (ASQ & SSQ); Alfred Kromholz (SSQ); Tim Rice; James M. Simpson (ASQ); Tom Starai (IEEE), Tom Neff (IEEE), Lance Kelson (SSQ & IEEE), Aaron Dagen (IEEE)

Sponsored Jointly By: The American Society for Quality (ASQ), Washington DC & Maryland Metro Section (509), Software Special Interest Group (SSIG); IEEE Computer Society, Washington, DC & Northern Virginia Chapters; and Society for Software Quality (SSQ), Washington, DC Area Chapter. Members of the **ASQ SSIG** include software quality professionals, software engineers, and others interested in applying quality principles to the field of software development. See our web page: <http://www.asq509.org/ht/d/sp/i/2499/pid/2499>. We meet every month, usually at the MITRE facility in Tyson's Corner, Virginia, with VTC to other locations.

Next Month: 'Smartphones (Android 2) in Foreign Wars: Locking Down Linux, Dalvick, Software Apps, and Accessories' by Jeffrey Voas of NIST, on Tuesday, March 27, 2012

Directions to the MITRE-2 Facility in McLean, Virginia:

Take the Beltway, I-495 to Virginia. Take Exit 46B (McLean, Route 123). Take Route 123 North, (also called Dolley Madison Blvd.) and go to the second traffic light at Colshire Drive. Turn right on Colshire Drive and continue through circle on Colshire. **Park in front of or to the right of the buildings, before passing the gate. (The gates are closed at 7:00).** Additional directions can be found at: http://www.mitre.org/about/locations/va_mclean_mitre2.html



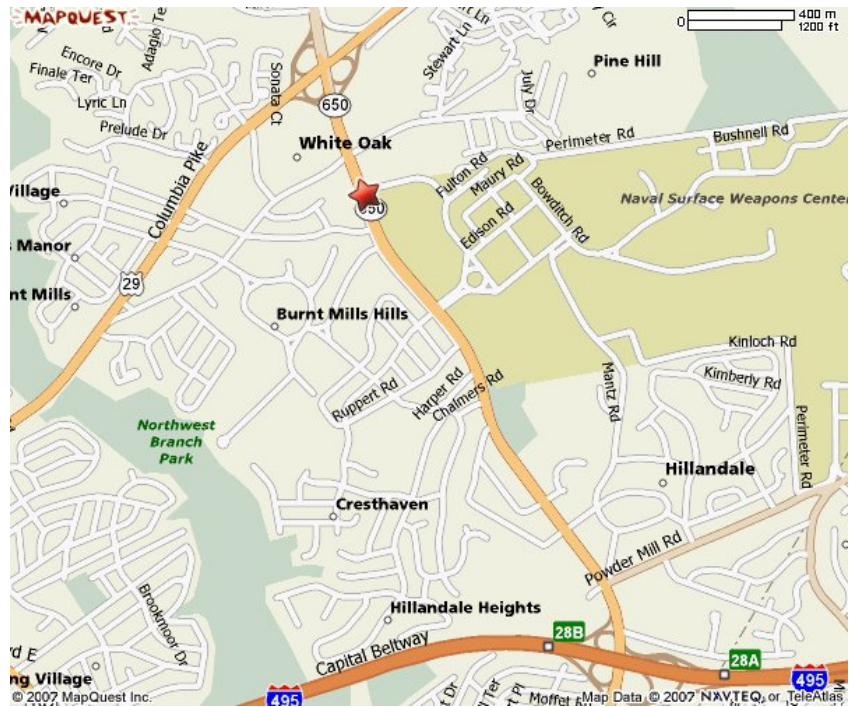
Directions to the FDA facility in Silver Spring, MD:

From the Capital Beltway, I-495, take New Hampshire Ave, Rt 650 north to Michelson Rd.

From Columbia Pike, Rt 29, take New Hampshire Ave, Rt 650 south to Michelson Rd

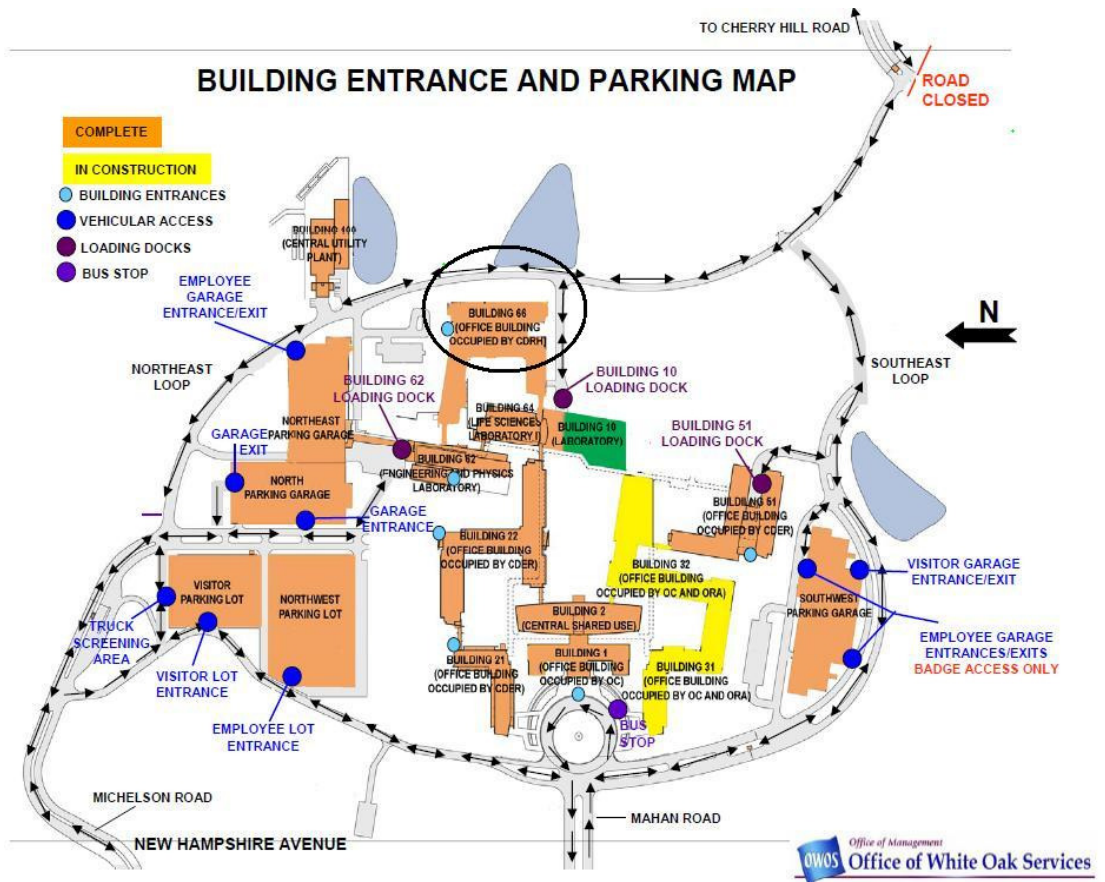
From the Capital Beltway, I-495, take New Hampshire Ave, Rt 650 north to Michelson Rd.

From Columbia Pike, Rt 29, take New Hampshire Ave, Rt 650 south to Michelson Rd



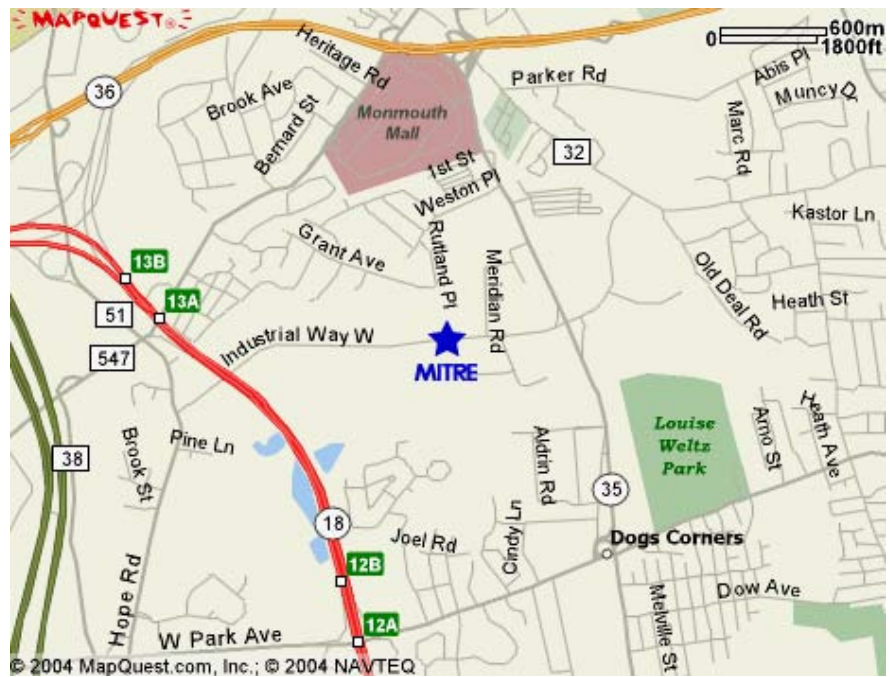
White Oak Building 66 (circled), room G512. This is a large conference room just beyond the Security desk on the right side of the grand atrium.

After 6 PM, visitors may use the surface parking closest to the building 66 entrance which are reserved for commuters with car pools. The north east parking garage is also an option.



Directions to the MITRE Facility in Eatontown, New Jersey:

From the New Jersey Turnpike If traveling from the **SOUTH**, get off the Turnpike at Exit 7A (195 toward Shore Points). Take 195 East towards the ocean and shortly after 195 turns into Route 138 (approximately 35 miles) watch for Route 18 North (Eatontown). Take Route 18 North to Exit 13A (Wayside West/Wyckoff Road). At end of ramp, bear left. At first traffic light (Hope Road) make a left turn. Make second left turn onto Industrial Way. The MITRE Corporation is next to the First Atlantic Credit Union on the left hand side of Industrial Way. There is a MITRE sign out front.



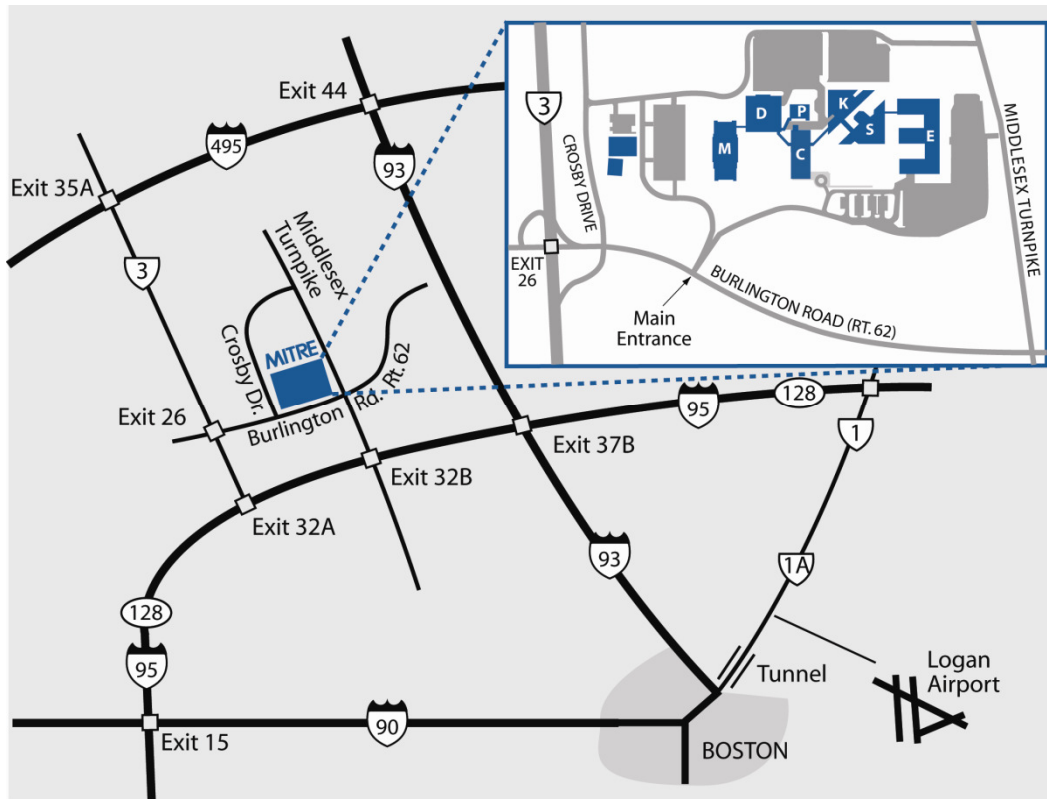
There are two buildings on the left side of Industrial Way. The first building is MITRE, the second building is TYCO. Take a left turn into the parking lot of the first building, which is MITRE.

If traveling from the **NORTH**, get off the Turnpike at Exit 11 (Garden State parkway exit). Follow the Garden State Parkway until Exit 105 (Eatontown). Follow the directions from the Garden State Parkway below.

From the Garden State Parkway: Follow the Garden State Parkway from the North or from the South to Exit 105 (the exit numbers increase going from south to north). After paying the toll at Exit 105, make first right turn onto Hope Road. Follow Hope Road to Industrial Way (second left turn after crossing Wyckoff/Shafto Road). Make second left turn onto Industrial Way. The MITRE Corporation is next to the First Atlantic Credit Union on the left hand side of Industrial Way. There is a MITRE sign out front. There are two white buildings on the left side of Industrial Way. The first building is MITRE, the second building is TYCO. Take a left turn into the parking lot of the first building, which is MITRE.

When you are facing the front of the MITRE building, the entrance to the ASQ meeting will be from the left parking lot opposite First Atlantic bank. Follow the signs to the conference room.

Directions to the MITRE complex in Bedford, Massachusetts:



From New Hampshire to MITRE Complex:

Take Route 3 South to Exit 26 (Route 62)

Turn Left on Route 62. It is a short distance to the MITRE entrance on left--watch for building directories on MITRE grounds

From Manchester Airport (NH) to MITRE Complex:

Start out going West on Airport Rd. toward parking

Turn slight right onto Brown Ave/NH-3A

Merge onto NH-101 West via the ramp on the left toward Bedford/Nashua

Take the Everett Turnpike South exit toward Merrimack/Nashua

Merge onto Everett Turnpike (toll road)

Everett Turnpike becomes US-3 South

Take exit 26 (Route 62) toward Bedford/Burlington

Turn Left onto (Route 62) Burlington Road

At second set of traffic lights, turn left at MITRE Bedford Campus entrance--watch for building directories on MITRE grounds.

Logan Airport to MITRE Complex:

Exit airport towards Route 1A South/Summer Tunnel (I-93) Boston.

Proceed through tunnel towards Storrow Drive (I-93 North).

Take I-93 North eleven miles to Exit 37B (Route 128 (I-95) South).

Take Route 128 (I-95) South six miles to Exit 32A.

Take Exit 32A, and proceed on Route 3 North.

Take Route 3 North for two miles to Exit 26 (Route 62).

Bear right on Route 62.

Take Route 62 a short distance to the MITRE Bedford Campus entrance on left--watch for building directories on MITRE grounds.