

Authorization depended on attributes, such as national identity, mission role and emergent situation.

At the beginning of the demonstration, each of the participants was issued sign-on credentials. Separately, a command authority predefined which information resources could be made available to which categories of consumers through a set of policies. The policies recognized several operational states (normal, emergency and self defense) and established different rules for each state. Participants accessed C2 resources through a Web site set up for the exercise. The Web site hosted authentication and authorization services, and governed user access based on the user's credentials and the policy for the prevailing operational situation.

Definitions of Operational Security Policies

As the trial scenario unfolded, intelligent software agents within the VIRT service looked for suspicious activity by monitoring ship tracks, meteorological and oceanographic (METOC) warnings, and UAV sensor data. If a ship's track data indicated a sudden course change, or a change with respect to national flag, or increased speed as it approached the three-mile limit of the U.S. West Coast, the VIRT service delivered a pop-up message to the appropriate watch officer's browser.

In response to this notification of an emergency situation, the watch officer immediately used a point-and-click menu to set emergency security policy. Because the situation demanded that non-U.S. coalition platforms interdict the threat, the policy authorized specific non-U.S. platforms to access the C2 portal to view local track and sensor data — data that would be withheld under normal conditions.

During the interdiction, intelligent software agents noticed a coalition interdiction platform in imminent danger of entering a mine field depicted on a SECRET NOFORN

METOC warning. Accordingly, the VIRT service delivered a pop-up message. The alert triggered the U.S. national watch officer to authorize the endangered foreign vessel for self-defense level of access. When the interdicting vessel avoided the hazard and intercepted the threat vessel, the coalition watch officer reset the security policy to normal.

In a June 2008 memorandum titled "Role-player after-action comments and observations," CWID sponsor feedback on the demonstration was overwhelmingly positive. "Each time the security policy was set to a different level, all users whose operating-picture views were supposed to change did see the appropriately updated picture ... The VIRT concept combines the best features of 'smart push' and 'demand pull' information management processes to provide probably the best shared, managed, situational awareness we can create right now ... Helped forward the development of access controls."

A logical next step was to test the capability with live data feeds — a test that took place in late February 2009 at the Naval Postgraduate School–SOCOM Exercise at Camp Roberts, Calif. The team successfully executed a follow-on experiment using Raytheon's Cobra UAV to demonstrate dynamic access control of the UAV's full-motion video. As before, the dynamic policy engine provided secure authorization of network services based on user-provided, preapproved credentials, and successfully demonstrated emerging access-control technology.

The W2COG and Raytheon demonstrated their commitment and know-how to provide combatant commanders with state-of-the-art, secure, interoperable coalition data sharing. ●

Jerry Pippins

jerry_l_pippins@raytheon.com

Contributors: David Minton, Paul Barré

Partnering with George Mason University on Secure Information Systems Research

Raytheon is working with researchers at George Mason University's (GMU) Center for Secure Information Systems to improve its ability to develop high-assurance systems. Current research and development activities include automating vulnerability analysis and hardening systems through secure virtualization.

Automating vulnerability analysis

CAULDRON (Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks) is a tool that GMU recently developed to automate vulnerability analysis, the task of examining network security to identify deficiencies and predict the effectiveness of proposed improvements. Vulnerability analysis is performed manually today. To perform this analysis, engineers must find the vulnerabilities that an attacker could exploit and the many paths that an attack could take in order to traverse a network and reach the attacker's target. This has become an intractable task, as systems and networks have grown more complex and as exploits have become more numerous. Given thousands of exploits, vulnerabilities and possible network configurations, vulnerability analysis needs to be automated.

An attack may penetrate a network at one node and then hop from that node to reach a target at a remote node in the network. A multistage attack may employ different exploits along the way, as different nodes may have different vulnerabilities. It may also traverse the network via many possible attack

Continued on page 36

Continued from page 35

paths. A vulnerability analysis should ideally identify all possible attack paths, and the exploits and vulnerabilities used to traverse them.

Once the attack paths and exploits are known, developers may add security mechanisms or reconfigure the network in order to “harden” the network. Proposed changes can then be analyzed to predict their effectiveness before they are implemented.

Multiple solutions can be explored at minimal cost if the process is automated.

Vulnerability analysis needs to be a continuing activity. Networks are dynamic places: they expand and are upgraded; new vulnerabilities are discovered, and so are new exploits. Each of these changes can affect the security posture of a network. By automating vulnerability analysis, CAULDRON makes it practical to periodically perform thorough

vulnerability analyses, and find and eliminate new vulnerabilities before an attacker finds and exploits them.

Figure 1 shows CAULDRON’s inputs. Commercial off-the-shelf tools provide information about network topology, known threats and intrusions. The user provides CAULDRON with attack scenarios that identify an attacker’s potential network entry point(s) and target(s). CAULDRON then

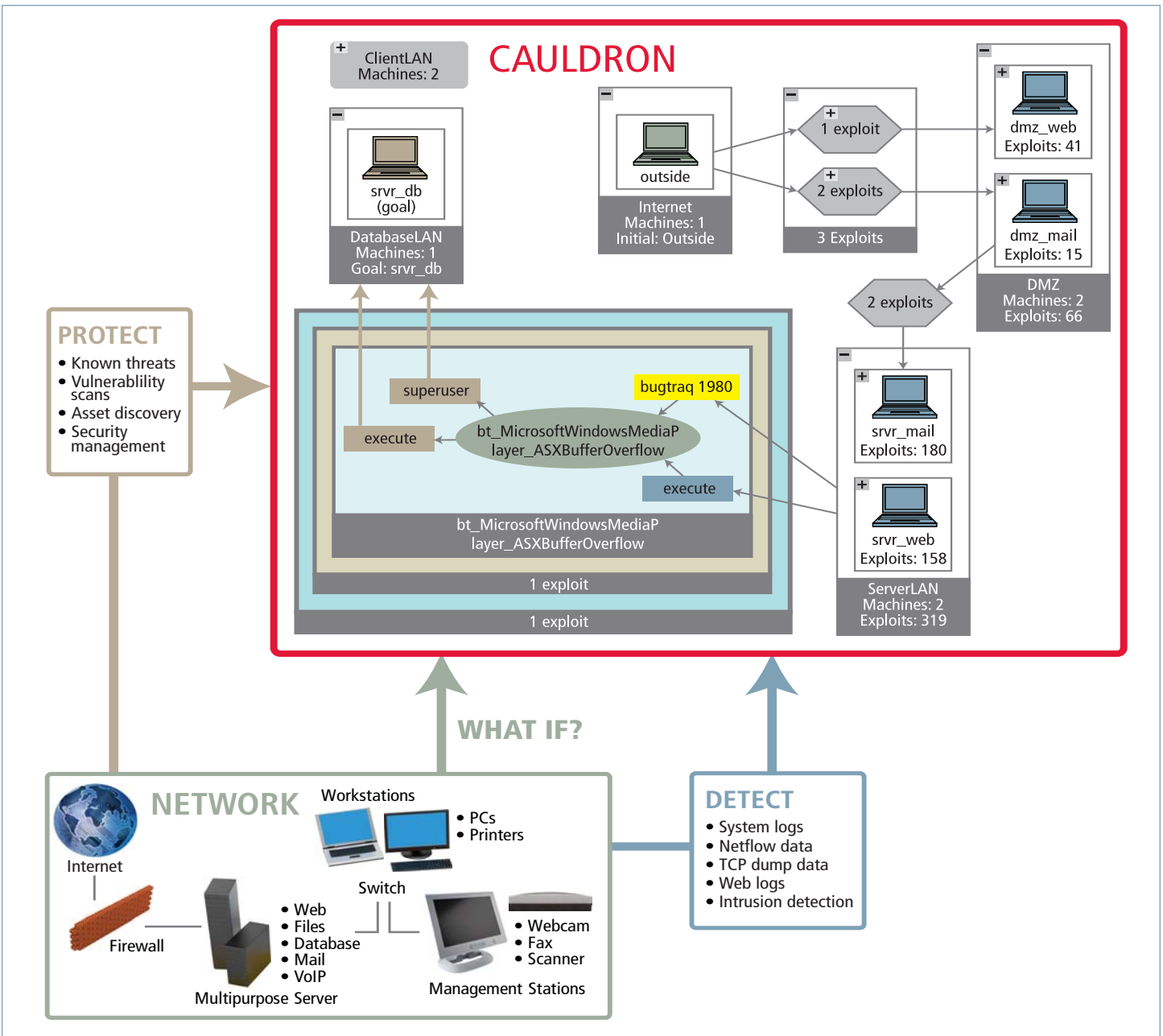


Figure 1. Inputs to CAULDRON

finds all of the paths and exploits that an attacker could use to reach those targets.

CAULDRON provides the user with visualizations of its analysis results, as shown in Figure 2. This gives the user information about attack paths, vulnerabilities, and exploits used, as well as recommendations for how network security can be effectively improved with minimal addition of security mechanisms. Raytheon has successfully used

being transitioned into Raytheon for further use as the technology matures.

Security Through Virtualization

Recent research has shown that virtual machines can be used to improve system security. The concept of a virtual machine has been around for many decades; it is a software implementation of a computer that executes a program like a real machine. For example, an application that runs on one

at GPU, it is transitioning into a commercial product offered by Secure Command. Raytheon is evaluating Internet Cleanroom for potential deployment in its own products and IT system.

The Uninterruptible Server is another technology that GPU is developing to protect servers from attack. It helps make servers intrusion tolerant, i.e., able to operate through an attack, even when the attacker

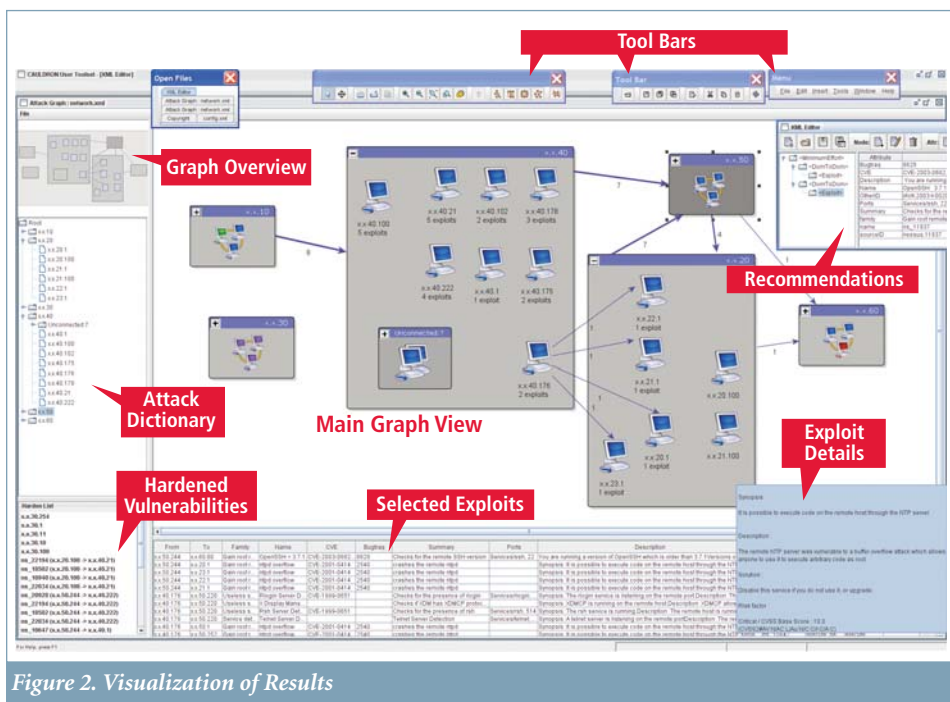


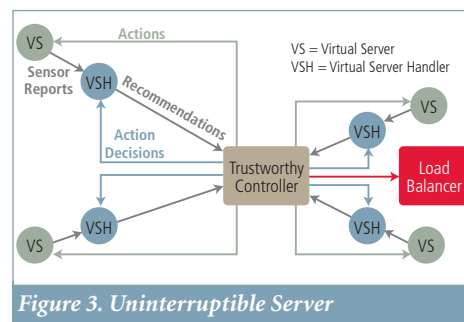
Figure 2. Visualization of Results

a beta version of CAULDRON on multiple engineering programs, both to evaluate its performance and perform vulnerability analysis.

On one of these programs, an 81-host system with more than 2,300 open Internet ports was analyzed for vulnerabilities. Current practice would have required engineers to manually interpret vulnerability scan data, find critical attack paths and eliminate critical vulnerabilities. This would have taken weeks to do. CAULDRON found the attack paths, identified the critical exploits, recommended solutions, and helped eliminate 75 percent of the vulnerabilities in a few hours. The technology is

operating system could also run on another operating system if a virtual machine were installed between the application and the second operating system. Security mechanisms can be combined with virtual machine technology to isolate a host computer from its applications in such a way that if an application is compromised, the application and its operating environment can be dismissed without harming the host computer or other applications.

Internet Cleanroom is one such technology. It protects hosts from Web-based attacks by running a browser or e-mail application on a virtual machine with mechanisms to detect and respond to compromise. Developed



has penetrated the system. The Uninterruptible Server runs multiple copies of server software on separate virtual machines, which are software emulations of the computers that run on real computers. As shown in Figure 3, each virtual server handles Internet service requests. A VS handler monitors each VS and makes local decisions to kill unauthorized processes that may appear due to Web-based attacks. Global decisions such as reverting servers are made by a trustworthy controller. A load balancer advertises a single IP address to the Internet and feeds Internet requests to the servers at random. The trustworthy controller is not addressable from the Internet side of the servers, so it is protected from Web-based attack.

Raytheon is working with GPU to adapt these technologies for use in Raytheon systems. ●

Tom Bracewell
bracewell@raytheon.com