

Divine Intrusion Protection

BY AL BERG

For centuries, Christians around the globe have prayed to Saint Jude, the patron saint of “impossible tasks.” The prayers of systems administrators who seek the “Holy Grail” of network security—an operating system that repels attacks even after perimeter security has been breached—may have been answered with the development of a divine new application.

Saint Jude LKM, a major topic of discussion at July’s Def Con in Las Vegas, is a Linux-based operating system add-on designed as a “last resort” defense against computer attacks. The application is implemented as a reference monitor directly into the operating system’s kernel. The software watches all operations and compares them to a rulebase that determines which makes sense from a security perspective. If an operation does not match one of the permitted actions for a particular application, Saint Jude stops the offending process. For example, if an attacker tries to gain control of a Web server by posing as a “nobody” user and tries to elevate his privileges to root, the attack program will be shut down before the operation finishes.

What does all this mean? In a nutshell, Saint Jude looks for processes that attempt to make unauthorized transitions into a root state, denying them free run of the system. The program takes the unsaintly action of terminating the offending processes with extreme prejudices. Unlike intrusion detection-type products, Saint Jude looks for the potential consequences of the attack, not just an exploit signature. It also does not rely on a database of known exploits—which are outdated as soon as someone thinks up a new attack.

Saint Jude is still under development by its architect, Tim Lawless, a systems administrator at the University of Southern Mississippi. The program, designed for Linux—and soon as a port for Solaris—is available from **Packetstorm** (<http://packetstorm.security.com>). Because the program is in the early development stage and hooks directly in to the OS kernel at a low level, Lawless recommends only using Saint Jude if you are aware of what it does and how it works. (Lawless also suggests contacting him first.)

Commercial vendor **Argus Systems Group** (www.argus-systems.com) is also making a big splash in OS security innovations

with its PitBull trusted operating system, which implements mandatory access controls on top of the Solaris 7 kernel. A PitBull-secured system won the BOFH (Bastard Operators From Hell) side of the annual Def Con Capture the Flag hacking contest by withstanding all attacks from attendees. PitBull takes a slightly different approach than Saint Jude by implementing many more gradations of access control at the operating system level. This denies attackers control of the system even if they obtain the root passwords. [Editor’s note: See www.infosecurymag.com/may2000/os_security.htm for the full PitBull story.]

Why are Saint Jude and PitBull news? Because they herald

new trends in intrusion protection technology and practices. Vendors and users are beginning to realize that firewalls and intrusion detection systems (IDSes) placed at network perimeters are not an adequate defense solution. Systems within the network borders need to be hardened against attacks, as well. Applications such as Saint Jude and PitBull are a part of the next generation of defenses. **ClickNet** (www.clicknet.com), with its interceptor IDS, and **Recourse Technologies Corp.** (www.recourse.com), with its ManTrap “honeypot” system, are two companies that offer similar products within this emerging “intrusion prevention” market.

Systems administrators and users need to realize the limits of signature-based defense applications. Hackers also read the trade rags and know that more and more of the networks they target

are only using traditional IDSes. In turn, the attackers are developing innovative methods for disguising their probes, exploits and attacks. Saint Jude and similar products provide protection even after an IDS has been fooled.

Attackers are becoming more sophisticated, and most systems continue to rely on limited measures, including usernames and passwords, to secure key corporate data. New approaches, such as Saint Jude and PitBull, throw up more aggressive defenses even after attackers breach conventional perimeter battlements. ▀

AL BERG (aberg@mentortech.com) is a consultant in the security practice of Mentor Technologies Inc.



ILLUSTRATION BY ROBERT BURGER