PEER PATCHING - RAPID RESPONSE IN DISTRIBUTED SYSTEMS

L Jean Camp
School of Informatics
901 E 10th Street
Indiana University
Bloomington, IN 47401

Allan Friedman
Harvard University
79 JFK Street
Cambridge, MA 02138
Allan_Friedman@ksgphd.harvard.edu

ABSTRACT

The Objective Force will require the defense of many different information systems on which it will depend. Addressing software vulnerabilities in the field, i.e., patching, requires discovery of vulnerabilities, communication of repair software, and installation of patches. Patch installation must occur without forcing interrupts under fire, downtime during critical tasks, or creation of new systemic vulnerabilities. Peer patching enables the necessary rapid review and dissemination of vulnerability repair without creating additional risk vectors.

INTRODUCTION

The army of the future will not only comprise soldiers and weapons systems, but also the information technologies that link these components together and allow unprecedented command and control capabilities. These supporting information technologies create new strengths, but also new risks and weaknesses (e.g., Denning, 1998; Slabodkin, 1998). Leveraging the capacities of a smart force requires enabling the force to both utilize and protect its software.

Vulnerabilities in supporting information technology can create an asymmetric threat if the technologies can be hijacked by less advanced adversaries. Adversaries can attack the software systems supporting combat and support units, as well as the units themselves. Therefore such units must be able to repair in the field, yet authorization to repair systems could be subverted to attack systems. The architecture of a networked battlefield demands a unique security support architecture known as *peer patching*.

Peer patching as proposed in this paper has three critical advantages. First, peer patching scales O(log n). Second, peer patching does not require contact with a centralized node. Third, relaying on conceptual biological models, peer patching does not create additional vulnerabilities. If systems can secure other systems in ad hoc networks, rather than relying on a centralized administrator, protection against vulnerabilities can be rapidly spread without creating a central target for an attacker.

PEER PATCHING: THREAT & DEFENSE

The Objective Force must address tactics designed to deny access to military services, as well as attacks against command and control nodes. Yet centralized distribution of software to address security vulnerabilities (i.e., patching) in the model of established commercial off-the-shelf technology (COTS) create targets for such attacks. COTS reliability has already been proven suboptimal for the workplace, much less the battlefield. (Marx et al, 2002). An attack against a command and control node as proposed in the *U. S. Army White Paper: Concepts for the Objective Force* has already been implemented by Blaster against COTS. Blaster, a worm discovered in August 2003, implemented a denial of service attack against windowsupdate.com, thus preventing the installation of the defensive Windows patch.

Network attacks have unique threat models. First, an attack can cripple a system not only by direct assault, but also by clogging the data channels. Most of the harms caused by recent internet worms, for example, were wrought by overwhelmed servers and clogged bandwidth that took entire corporations offline. Furthermore, an adversary can attack remotely,

Jean Camp & Allan Friedman, "Peer Patching – Rapid Response in Distributed Systems," *24th Army Science Conference* (Orlando, FL) 28 November – 2 December 2004.

and possibly invisibly. Traffic can come from any part of the network, including compromised machines that were previously friendly. Finally, absent the ability to communicate to a central server, a client may lose not only immediate functionality, but also the ability to arm itself against further attack.

The necessarily ad hoc nature of the battlefield network means that some units will be out of contact at some time: if they failed to acquire the necessary defenses before disconnection they would remain vulnerable. (Toh et. al, 2002). A decentralized system is necessary to ensure that the requisite defensive measures can reach as many systems as possible in a timely manner.

Yet decentralized user-centered repair of vulnerabilities can itself be used as an attack vector. (Anderson, 2001) The Sober and Swen worms disguise themselves as a patch from Microsoft in order to convince users to install malicious code. Phishing and other human engineering attacks have been effective at subverting users attempts to secure themselves. Even absent human engineering, users may not be unable to select the appropriate defense. For example, most users were unaware of their vulnerability to Slammer as it attacked the underlying SQL database in MS Office, and users were unaware of the existence of the SQL code.

Peer patching exploits the same vulnerability that an attack might use. A network attack occurs when machine exploits a software bug such as a buffer-overflow error to obtain permissions otherwise unobtainable, and then to run malicious code. Peer patching uses the vulnerabilities to run friendly code. If the friendly attack from the peer fails, the attacked system is not vulnerable. If the attack is successful, the system executes patching code on the vulnerable machine, closing the vulnerability and protecting the peer system from a malicious attack. The peer-patching software on the newly patched peer than seeks to secure its own peer machines.

Peer list can be assigned centrally as each system joins, dynamically through network interaction, or some combination of the two, much like peer-to-peer search mechanisms. (Kalogeraki etl al, 2002). The underlying network substrate can vary, as long as packets or cells from one device can reach another.

Peer patching assumes only the existence of communications between vulnerable systems. It requires the creation of the patches themselves. Once created, the patches can be released to a few select machines, and from there can spread rapidly across the peer lists. The number of patched machines will grow exponentially, yet no one machine will be overloading its local communications channel. With no user involvement, an entire network of machines can be patched very quickly, without relying on the availability of a single, centralized server. Peer relationships are reciprocal so the patches can flow throw the network in any direction. Systems continue to attempt connections that they cannot reach, so that when a mobile system reconnects with the larger network it can be patched quickly.

Note the software clients may be lowest priority, so that patching never interferes with priority actions or interrupts critical processes. The critical element for peer patching will be a timing mechanism to ensure that the peer patching system does not exhaust batteries or flood communications channels when the system is operating at peak capacity.

CONCLUSIONS

Network defense in a modern warfare environment requires constant vigilance, rapid deployment and a decentralized architecture.

Peer patching provides critical features based on observations of biological systems to enable reliable system repair. Peer patching uses existing vulnerabilities to repair those same vulnerabilities. Peer patching builds on social networks to ensure duplicate paths to any individual hardware element.

Peer patching supports the mission of the Army by enabling high-speed, effective, real-time network response to a vulnerability as soon as a patch is made available. By exploiting the very vulnerability that poses the original security risk, it introduces no new threats or weak points into the system. It rides on top of existing networks, and is designed explicitly to work with commercial off-the-shelf technology.

REFERENCES

Anderson, R., 2001: *Security Engineering* John Wiley & Sons, 640.

Denning, D., 1998: *Information Warfare*. Addison-Wesley, 552.

Kalogeraki, V., Gunopulos, D., Yazti, Z., 2002: A Local Search Mechanism for Peer-to-Peer Networks *Proceedings of the eleventh international conference on Information and knowledge management* 2002

Marx, W. J., Strickland B. R., Lianos D, 2002: Miniature Smart Munitions/Guided Projectiles for the Objective Force *Army Science Conference,* Orlando, FL 2002

Toh, C-K. et al, 2002: "The Design and Implementation of Next Generation Tactical Ad Hoc Mobile Networks" *Army Science Conference,* Orlando, FL 2002