Chapter XI

Experiences Enhancing Open Source Security in the POSSE Project

Jonathan M. Smith, University of Pennsylvania, USA
Michael B. Greenwald, University of Pennsylvania, USA
Sotiris Ioannidis, University of Pennsylvania, USA
Angelos D. Keromytis, Columbia University, USA
Ben Laurie, AL Digital, Ltd., USA
Douglas Maughan, Defense Advanced Research Projects Agency, USA
Dale Rahn, University of Pennsylvania, USA
Jason Wright, University of Pennsylvania, USA

ABSTRACT

This chapter reports on our experiences with POSSE, a project studying “Portable Open Source Security Elements” as part of the larger DARPA effort on Composable High Assurance Trusted Systems. We describe the organization created to manage POSSE and the significant acceleration in producing widely used secure software that has resulted. POSSE’s two main goals were, first, to increase security in open source systems and, second, to more broadly disseminate security knowledge, “best practices,” and working code that reflects these practices. POSSE achieved these
Experiences Enhancing Open Source Security in the POSSE Project

goals through careful study of systems ("audit") and starting from a well-positioned technology base (OpenBSD). We hope to illustrate the advantages of applying OpenBSD-style methodology to secure, open-source projects, and the pitfalls of melding multiple open-source efforts in a single project.

INTRODUCTION

Posse - a group of people summoned by a sheriff to aid in law enforcement.

A variety of reasons, ranging from marketplace ignorance to a perceived trade-off between usability and security, have driven modern operating systems into the undesirable role of a potential lever with which system security can be breached. The use of any common operating system platform across an organization can make this lever effective, independent of the organization, its security policy, and security practices.

This problem has been exacerbated by the commercial success of the Internet over the last decade, as the Internet’s “end-to-end” (Clark, 1988; Saltzer, Reed, & Clark, 1984) design implicitly relies on host security as the basis of security for the overall system. An example of this reliance and its consequence is the advent of Distributed Denial of Service (DDoS) attacks, effected by multiple computers bombarding one or more target hosts with traffic and disabling these targets.

As the commercial marketplace, and to a large degree the government marketplace, have converged towards a common platform (the dominant commercial operating system, Microsoft Windows), these organizations increasingly rely on the platform to be trustworthy, whether it is so or not. Further, the use of the Internet and computer systems in the functions of all of these organizations has made systems software, as a whole, “critical infrastructure.” At the same time, a single point of vulnerability and failure has been created for systems dependent on this software.

The Open Source Alternative

Concurrent with the growth of the Internet, an alternative software development paradigm began emerging. This paradigm had roots in the research UNIX community and its USENET, with some philosophical roots later added with the “Free Software” principles of Stallman. The mid-1960s MULTICS (Daley & Dennis, 1968; Organick, 1972) project, part of the U.S. Defense Advanced Research Projects Agency (DARPA)-supported Project MAC (Fano & David, 1965) at MIT, gave rise to the original UNIX system (Ritchie & Thompson, 1974, 1978; Thompson, 1978) (the name UNIX is in fact a pun on MULTICS) as a reaction to MULTICS system complexity. Unfortunately, in rejecting much of MULTICS, the UNIX system was not able to avail itself of the extensive effort devoted to developing protection models and security kernels (Schroeder, 1975; Schroder, Clark, & Saltzer, 1977) for
Related Content

Action Potentials: Extrapolating an Ideology from the Anonymous Hacker Socio-Political Movement (A Qualitative Meta-Analysis)
www.igi-global.com/chapter/action-potentials/120944?camid=4v1a

A Framework for Understanding the Open Source Revolution
www.igi-global.com/article/framework-understanding-open-source-revolution/38902?camid=4v1a

The License Choices of SMEs doing Business with Open Source Software: Empirical Evidence on Italian Firms
www.igi-global.com/article/license-choices-smes-doing-business/75521?camid=4v1a
Effort Estimation
[www.igi-global.com/chapter/effort-estimation/36505?camid=4v1a](www.igi-global.com/chapter/effort-estimation/36505?camid=4v1a)