Securing your IT with open source

Vlatko Košturjak, IBM

IT infrastructure is critical infrastructure of every organization. Therefore, it is obvious that it must be well protected. As we all know, IT security is not just technology, it applies to all aspects of protecting information and data. It includes processes, organization and execution. In one word - it is a never ending story. We will focus on technical problems regarding IT security and how open source tools and applications can help in such a protection.

From a technical standpoint of view, first step toward securing infrastructure is tightening security of IT infrastructure itself. In that step we try to secure our infrastructure according to existing laws, regulations and policies. Although, this step is mostly done by hands, we can automatize it with scripts. Also SELinux, Grsec and Bastille can help in hardening operating system.

Monitoring and preventing process includes monitoring data or information flow while preventing unauthorized access. For basic monitoring of network, we can use MRTG, SmokePing and BigBrother. Snort, Argus and Bro IDS can help in developing network intrusion detection system (NIDS), while tools like Samhain, Tripwire, Lml and systrace can help in developing host intrusion detection system (HIDS). For integrating NIDS and HIDS data we often use Prelude which is Hybrid intrusion system (HyIDS). Rrdtool can be used to customize monitoring if there's something else we wish to monitor. Mon, Openms and Nagios are general monitoring systems. For step forward i.e. Implementing prevention system we can use BlockIT or Snort2pf for preventing of intrusion or we can write and customize existing scripts. For implementing wireless intrusion detection system and prevention we can use Widz, Kismet and Fake AP. We can choose between OS-SIM and Demarc for integrating all those security informations.

Forensic comes when hardening, monitoring and preventing processes fail. Although, this step nobody likes because we think somebody outsmarted us, it is a time when we learn a lot. Cheer up! Next time, hardening will include lessons learned :) In this process, we can use data gathered from log files, IDS and other security mechanisms to find out what and where happened. There's plenty of forensic bootable CD's which we can use for forensics. Tools like Sleuth and Coroner's Toolkit are often found on such a CD's.

From author experience we can say that new and promising as well as well-known and popular open source tools can help in every mentioned process. There are plenty others on the Internet and it is hard to decide which one is suitable for specific situation. Challenge is not just a finding suitable tool, challenge is actually in integrating them with goal to automatize all security processes we have.

For better integration, it is more than obvious that open standards are prerequisite for any advanced security mechanisms. There is Intrusion Detection Message Exchange Format from IETF which is already used in most tools mentioned. But for next step towards autonomic computing, it is necessary to implement in every mentioned tool standards like OpenSec's Advisory and notification markup language (ANML), System information markup language (SIML) and Software description markup language (SDML). So, smile! Fact that standards like ANML, SIML and SDML already exist

means that future is bright!