Chapter 10

E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems

Harold Pardue
University of South Alabama, USA

Jeffrey Landry
University of South Alabama, USA

Alec Yasinsac
University of South Alabama, USA

ABSTRACT

Approximately 25% (according to http://verifiedvoting.com/) of voting jurisdictions use direct recording electronic systems to record votes. Accurate tabulation of voter intent is critical to safeguard this fundamental act of democracy: voting. Electronic voting systems are known to be vulnerable to attack. Assessing risk to these systems requires a systematic treatment and cataloging of threats, vulnerabilities, technologies, controls, and operational environments. This paper presents a threat tree for direct recording electronic (DRE) voting systems. The threat tree is organized as a hierarchy of threat actions, the goal of which is to exploit a system vulnerability in the context of specific technologies, controls, and operational environment. As an abstraction, the threat tree allows the analyst to reason comparatively about threats. A panel of elections officials, security experts, academics, election law attorneys, representatives from governmental agencies, voting equipment vendors, and voting equipment testing labs vetted the DRE threat tree. The authors submit that the DRE threat tree supports both individual and group risk assessment processes and techniques.

INTRODUCTION

Voting systems function to capture voter intent and anonymously convert that intent into tallied votes. Accuracy and secret ballots are fundamental to democracy. However, ensuring the accuracy of a tally and the anonymity of a voter is extremely difficult in electronic voting systems because the processes occur through a complex interaction of software, hardware, networks, people, policies and legislation (Jones, 2005; Khono, Stubblefield, Rubin, & Wallach, 2004; Weldemariam, 2009; Yasinsac & Bishop, 2008).
The voting system literature is replete with examples of attacks to electronic voting systems (Calindriino et al., 2007; Dill, Mercuri, Neumann, & Wallach, 2008; Epstein, 2007; Feldman, Halderman, & Felten, 2006; Fischer, 2003; Frisina, Herron, Honaker, & Lewis, 2008; Gardner et al., 2007; Hasen, 2000; Hursti, 2006; Kohno, Stubblefield, Rubin, & Wallach, 2004; NIST, 2005; Norden, 2008; Ohio Secretary of State, 2003; Yasinsac et al., 2007).

A pivotal aspect of ensuring integrity of elections conducted on DREs is that, because there is no physical record of each voter’s selections, security is dependent on the DRE software. Software is inherently complex. Theory shows that it is impossible to prove non-trivial properties about arbitrary programs (Rice, 1953) and that at best, testing “… can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence” (Ditkritra, 1972).

Was that not bad enough, it is also very difficult even to determine if a computer is executing the intended software (Thompson, 1984). Thus, even if a DRE is properly built, configured, and operated, anyone with private access to the device may be able to install malicious software (i.e., malware) that can alter or control election results.

There are many approaches to securing electronic voting systems: due diligence, compliance, and business enablement (Parker, 2006). Another means of securing voting systems is to conduct a risk assessment. Risk assessment involves assigning a quantitative or qualitative value to the risk of a threat in a specific situation. Assigning a value to the risk of a threat allows the analyst to judiciously allocate relatively scarce resources, conduct sensitivity analysis, perform cost-benefit analyses, and compute residual risk. One approach to conducting risk assessment involves threat trees (Schneier, 1999; Pardue, Landry, & Yasinsac, 2009; Yasinsac & Pardue, 2010).

A threat tree is an abstraction that models threat source/vulnerability pairs as a hierarchy of threat actions. Threat actions denote the means by which a threat source exploits a vulnerability or how a vulnerability is accidently exploited through a sequence of events or failures. A vulnerability can be defined as a “flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited to accomplish a security breach or a violation of the system’s security policy” (Stoneburner, Goguen, & Feringa, 2002).

The purpose of this paper is to describe a threat tree for DRE voting systems. By being an abstraction, a threat tree allows the analyst to reason comparatively about threats to electronic voting systems. That is, the analyst can reason comparatively about different hardware and software configurations, different types and sizes of elections, different controls, and different types of attackers. By organizing a threat as a hierarchy of threat actions, it informs the risk assessment process. That is, the analyst is able to define, in precise terms, the specific threat that is under consideration and can assign metrics that describe the cost and impact of a threat if successfully executed. It should be noted that the DRE threat tree presented in this paper is not presented an exhaustive or definitive catalog of threats to DRE voting systems. The DRE threats cataloged consider computer-based technology used inside of polling places and brought outside for curbside voting. The use of voter verified paper trails are not considered.

A Direct Recording Electronic Voting Machine (DRE) is a VotingMachine that conducts Voter-Interaction, VoteCommitment, and VoteCapture; Counts each Vote; and generates a persistent Ballot Image based on VoterInteraction. The essence of its name is that a DRE captures and records each voter’s selections electronically, with no need for a paper ballot. The most common DRE architecture uses touch screen technology for voter interaction, presenting each contest on the screen and allowing the voter to “touch” their selection. Voting integrity activists decry use of DREs because of the absence of physical records. Conversely,