Threat Modeling and Data Sensitivity Classification for Information Security Risk Analysis

Secure Electronic Elections – Case Study

Conference on Data Protection

December 2003

Belgrade, Serbia and Montenegro

Goran Obradović

Director of Technology

Chief Information Security Officer

goran@dvscorp.com

Agenda

- *Problem Statement*
- *Anti Patterns in Info Security Practice*
- *Info Security Risk Analysis – The Journey*
- *Threat Modeling with examples in Electronic Voting Systems*
- *Current state-of-the-art electronic election systems*
- *Conclusions*
- *Q & A*

DOMINION VOTING SYSTEMS

Problem Statement

It is not acceptable that only technical part of the team defines security requirements. Business stakeholder must be involved.

Events = Threats

Causes = Vulnerabilities

ROSI = Return on Security Investment

- *To secure an application or a system without spending excessive time and effort we are tempted to blindly apply security controls that have already been extensively used in practice*
- *However, without understanding security requirements common security controls can not provide adequate protection within the specific context*
- *We have to understand:*
  - *the real value of information resources that we need to protect*
  - *if an attacker has an interest to compromise our system*
  - *what are the events and causes that will have an unwelcome consequence upon our system*
  - *what will be risk mitigation techniques that will maximize our ROSI index and minimize overall threat probability or risk to an acceptable level*

DOMINION VOTING SYSTEMS