**Threat to voter privacy with voter verified paper audit trail voting systems using spooled paper rolls**

**Taxonomy:** Retail, vote buying or voter intimidation
**Applicability:** DRE voting systems with voter verified paper audit trail capability using spooled paper rolls that remain intact (uncut) post-election

**Method:**
This is an attack on voter privacy that is possible when using a DRE with a voter verified paper audit trail capability that uses a spooled paper tape to record the voter's choices. The spooled paper tape records each voter's choices in the same order as voters using the DRE.

This attack is relatively simple: The perpetrator watches the order in which people use a particular voting system and notes the order of each particular vote he is interested in. At some point after the election, the perpetrator or a counterpart obtains the paper tape and compares the order of ballot records with the order of individuals who used the voting system on Election Day.

This attack could be used to enforce vote selling, or simply to invade the privacy of voters and determine how particular individuals voted.

**Resource requirements:**
If the purpose of the attack is to sell votes, the perpetrator must have access to a pool of subvertable voters willing to vote in return for payment or unable to complain if threatened. The perpetrator must also watch the order in which people use the voting systems, which could be done rather easily by using a hidden camera. To get access to the voting system's paper tape, the perpetrator must have access to the voting system post-election. This could occur in a number of ways, including subverting the physical security of the voting systems or by cooperation with a dishonest election official.

**Potential gain:**
One vote per subverted voter.

**Likelihood of detection:**

If the purpose of the attack is to sell or coerce votes, it depends on the degree of dependency linking the perpetrator to the subverted voters. It also depends on the ability of the perpetrator to take the paper tape, examine it, and then replace it without detection. Some paper tape units are sealed and provide some physical tampering indications; however a skilled and determined perpetrator could likely overcome these obstacles. Election officials may not be in a position to detect evidence of tampering or may attribute it to accident.

**Countermeasures:**
Appropriately-strengthened physical security on the election systems post-election will reduce the risk of this attack succeeding, unless the perpetrator is working with a co-conspirator who has physical access to the voting system. Use of tamper-resistant paper tape units that offer a very reliable physical indication of tampering would help. Also, cutting each ballot record from the paper spool will help to randomize the order of ballot records, thereby making the attack extremely unlikely to succeed.

**Citations:**
The risk of this attack has been cited frequently in newspaper articles, testimony on voting system security, and in many voting system research publications.

**Retrospective:**
Several voting system vendors use spooled paper rolls to record voter's ballot choices. The use of spooled paper tape units presents a dilemma, since the units if intact may be significantly easier to handle than separate sheets of paper or pieces cut from a paper spool, and therefore may have greater integrity associated with them. On the other hand, they represent a threat to voter privacy that can only be mitigated by tamper-resistant units and strong election procedures.