OWASP Risk Methodology: E-Voting adaptation of the Likelihood scale

The OWASP Risk Rating Methodology [1] is an approach to quantify the risk of security threats in order to make informed decisions. It evaluates the risk as the product of *likelihood* – i.e., how likely/easily a vulnerability is discovered and exploited by an attacker – and *impact* – i.e., material and non-material damage, such as the loss of data integrity or the reputation damage.

The provided factors to estimate the likelihood are connected with the worst-case threat agent (skill level, motive, opportunity, and size – i.e., from a specific developer to anonymous Internet users) and the exploited vulnerability (ease of discovery, ease of exploit, awareness, and intrusion detection – i.e., from active detection to not logged).

Likelihood To tailor the OWASP Risk Rating methodology to e-voting, considering the coercion scenario, we propose the following **likelihood factors** (scale 1 to 9):

- *Skill Level.* How technically skilled is a coercer (the lower it is, the easier it is to attack the voter): we consider a value of (8) if an asset is disclosed by physical observation or by simply requesting it from the voter; (7) if the coercer needs to access a voter's device or the asset is not visible in the set of actions to cast a ballot; (5) if the coercer is able to access a communication channel to/from the voter's devices; (3) if the attacker can perform combined attacks (such as learning voting intentions via social engineering and the vote expressed via an over-the-shoulder attack).
- *Motive.* How motivated is the coercer, in particular how well the attack could enable voter monitoring and control. We propose a rating of (2) if the monitoring is not specifically on ballot casting and has low probability of being successful, (4) if it still succeeds with low probability but directly linked to voting operations, (8) if the attack would give some direct control over voting capabilities. Intermediate values should be used to adapt for higher success probabilities or monitoring that allows the coercer to detect coercion evasion strategies (for example requesting a ruse PIN).
- *Opportunity.* What resources and opportunities are needed to perform the attack: we use (3) if the coercer needs to tamper with an external software supposed to be secure (e.g., a credential manager used by the voter); (4) if the attacker needs to know when the voter device will communicate (in order to attack); (5) if the attacker has to be able to attack a voter in two or more different time frames; (6) if the attacked asset can be retrieved by simply observing the voter but not during a compulsory operation (e.g. during an optional verification) (7) if the attacked asset is visible on the device during one of the operations necessary to cast a vote.
- *Ease of Exploit.* How easy is it for this group of threat agents to actually exploit this vulnerability. Here we follow the OWASP rating: theoretical (1), difficult (3), easy (5), automated tools available (9).

– *Evasion of Attack Detection* (named Intrusion detection by OWASP). We use (3) if the voter is promptly alerted or the attack is easily noticeable (e.g., they realise to have lost the voting device); (6) the voter may not realise to have been attacked if proper care has not been used (e.g., by not leveraging optional security mechanisms such as verification steps); (8) the attack can easily go unnoticed (e.g., in case a coercer passively listens on communication channels).

Since our main focus is the coercer, we do not quantify the *Size* factor. Considering its attack vectors (over-the-shoulder and social-engineering) we also do not consider *Ease of Discovery* (i.e., how easy an attacker discovers this vulnerability) and *Awareness* (i.e., how well known is this vulnerability to the attacker). Intermediate values (such as a skill level of 4) are assigned by comparison among similar attacks (or vulnerable assets), and lastly by using the values from the OWASP methodology (e.g., skill level 1 indicates no technical skills). The overall likelihood of each identified threat is computed as the average value of all the considered factors.

References

1. OWASP: Risk rating methodology, https://owasp.org/www-community/OWASP_Risk_Rating_Methodology