Security & Transparencies in E-procurement

Prof. E. Sreenivasa Reddy
Principal
University College of Engineering
Acharya Nagarjuna University
What is a threat

• Threat is a potential violation of security. The violation need not actually occur for there to be a threat.
• The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks.
• Those who execute such actions, or cause them to be executed, are called attackers.
Threats identified

• E-tendering system security policies define a subset of actions that transform etendering system from one secure state to another. Threats and possible security violations define the subset of actions that transform the e-tendering system from secure to insecure states.

• Identifying system threats is a complicated issue. It involves an overall understanding of the traditional business, legal requirements, technology (for example software applications), security standards for developing and maintaining a system, and fundamental computer security concepts.

• Major threats are present at each key step in the tendering process: pre-qualification and registration, public invitation, tender submission, close of tender, tender evaluation, award of tender and archiving.

• The normal system development requires that the developer identify threats and then define the system security requirements (Bishop 2003).
Threats

• The threats identified can be classified into the following categories:
  • Integrity violation
  • Confidentiality violations
  • Masquerading or impersonation
  • Repudiation
  • Time integrity violations
  • Non-verifiable evidence
  • Denial of service.
Integrity Violations

- It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- The integrity security requirement is essential to ensuring the correct execution of the e-tendering process as integrity violations can occur throughout most steps of the e-tendering process.
- To address integrity violations the integrity of transmitted messages must be protected.
- Also the integrity of documents must be ensured while stored temporarily in the tender box, Security and Legal Issues in E-tendering
- During evaluation and after the tender has closed. The integrity of different types of documents must also be maintained.
- Tender submission documents are obvious targets. But system logs and acknowledgement messages must also have their integrity maintained
Confidentiality violation

• Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.

• Like the integrity security requirement, confidentiality is essential to ensuring the correct execution of the e-tendering process.

• Confidentiality of messages is important when advertising closed tenders, submitting tender documents and conducting any post tender close negotiations.

• Confidentiality of tender documents, particularly tenderer submitted documents may also need to be maintained after the tender process has completed.
Masquerading

**Masquerade** is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.

This threat has lead to two security requirements.

1. The most obvious is the authentication of messages transmitted during the e-tendering process. False messages should be easily identified and rejected by all e-tendering parties.

2. The other is the authentication of user identities when accessing e-tendering computer systems. This is particularly the case when accessing the tender box application. Only authorised personnel should be gaining access to submitted tender documents.
Repudiation

- **Repudiation** means the act of claiming that something is invalid.
- The non-repudiation of messages and documents is another security requirement of etendering systems.
- Originators of messages and authors of documents should not be able to deny their part in the e-tendering process. The non-repudiation property is closely linked to authentication.
Time integrity violation

• Secure time is an important requirement in e-tendering.
• All tenderers and the principal should be operating with the same time thus all system clocks should be synchronised.
• This is particularly important given that the close of tender time is very important to the tender process. The authentication of the server that e-tendering parties synchronise with is also essential to prevent the wrong time from being set.
• Secure time-stamping is also an important quality when recording and logging e-tendering events.
Non verifiable evidence

• The secure record-keeping requirement addresses the threat of non-verifiable evidence.
• This requirement is linked with the integrity, confidentiality, authentication and nonrepudiation security requirements.
• If records are kept with these properties in mind the threat of non-verifiable evidence is greatly reduced.
Denial of service

- The availability of systems is a concern at all steps of the e-tendering process. But it is particularly important during the tender submission stage before the close of tender time. It is essential that the tender box be available for this time. Security and Legal Issues in E-tendering
Transparencies

- UNNECESSARY PROCUREMENT.
- TAILOR MAKING THE SPECIFICATIONS.
- ENTRY BARRIERS – NOT ALLOWING ELIGIBLE BIDDERS TO PARTICIPATE.
- NOT GIVING ADEQUATE PUBLICITY.
- NOT UPDATING LISTS OF APPROVED SUPPLIERS/CONTRACTORS.
Transperencies

- NOT MAKING TENDER DOCUMENTS AVAILABLE TO ELIGIBLE BIDDERS.
- MANIPULATIONS IN TENDER EVALUATION PROCESS.
- UNNECESSARY NEGOTIATIONS.
- ALTERING THE TERMS OF TENDER THUS FAVOURING CERTAIN CONTRACTORS/SUPPLIERS.
▪ UNDUE FAVOURS AT EXECUTION STAGE.
▪ INTENTIONAL DELAYS IN MAKING PAYMENTS AS MAIN SOURCE OF CORRUPTION.
▪ CORRUPTION IN HANDING OVER PAYMENT BY CHEQUES.