INEL-95/00599
CONF-960270--1

Improving Tag/Seal Technologies: the Vulnerability Assessment Component[a]

James L. Jones

Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, ID 83415

ABSTRACT

The Department of Energy (DOE), specifically the Office of Nonproliferation and National Security, has sponsored the development of numerous tag and seal technologies for high-security/high-valued applications. One important component in this technology development effort has been the continuous integration of vulnerability assessments. The Idaho National Engineering Laboratory (INEL) has been the lead laboratory for vulnerability assessments of fiber-optic-based tag/seal technologies. This paper presents a brief historical overview and the current status of the DOE high-security tag/seal development program and discusses INEL's adversarial role and assessment philosophy. Verification testing criteria used to define "successful" tampering attempts/attacks are discussed. Finally, the advantages of integrating a vulnerability assessment into the development of commercial security tag/seals are presented.

1. Introduction

During the mid-1980's, DOE used its national laboratory resources to initiate a tag/seals development program, which produced an array of novel, high-security tag/seal technologies[1]. The technologies supported arms control applications related to treaty verifications; specifically applications for nuclear weapon controls. Each tag/seal technology had to provide two basic functions: 1) uniqueness ("tag") and 2) some form of tamper indication ("seal") which could not easily be circumvented. In most cases, a technology included a tag/seal device to be applied to a fielded object, and an auxiliary, field-portable device for "reading" the tag/seal signature. The "reader" was assumed to be controlled by the inspector and brought to the field for each inspection. The tag/seal signature would enable an inspector to verify the device's uniqueness and, in many cases, confirm its sealed integrity.

During the Cold War, policy makers thought that treaty signatories could apply sophisticated tamper methods to any tag/seal device so as to circumvent compliance with any established treaty agreements. To address this concern, DOE embarked on a tag/seal development program. Continuous vulnerability assessments were integrated throughout the technology development

[a] Work supported by the U.S. Department of Energy, Office of National Security and Nonproliferation, under DOE Idaho Operations Office Contract Number DE-AC07-94ID13223.

process. Until this program was critically affected by the end of the Cold War in the early1990's, it was being expanded to include devices developed by the Department of Defense and had begun performing field demonstrations of selected technologies[2].

In almost every case, the tag/seal technology development process was impacted by these continuous vulnerability assessments. In most cases, vulnerabilities were identified, modifications were made, and an improved technology resulted. In some cases, the entire technology development effort was discontinued. Today, largely because of the DOE tag/seal program with its integrated vulnerability assessments, many of the tag/seal technologies continue to be applicable to numerous domestic and international safeguards requirements.

2. INEL's Assessment Role

Lead laboratory status for tag/seal adversarial assessments were selected based on each laboratories particular expertise. INEL was selected as the lead laboratory for vulnerability assessments of all fiber-optic-based tag/seal technologies because of its capabilities in fundamental engineering design, systems evaluation, testing expertise, and fiber-optic applications development.

From the onset of the DOE tag/seal program, INEL's adversarial role could most accurately be described as that of an "independent collaborator." In many cases several technologies from different national laboratories and non-DOE agencies were assessed simultaneously. These interactions resulted in a very successful forum for multi-laboratory and multi-agency cooperation and were highly effective in enhancing the overall tag/seal development process.

Despite the strong collaborative interactions, the independent nature of the assessments was never compromised. All INEL vulnerability assessments were performed at INEL. Except for the tag/seal technologies themselves, all equipment used was owned by INEL and all attack methodologies were devised by INEL. Assessment results were formally presented at semi-annual meetings or through established DOE channels.

3. Adversarial Philosophy

The objective of these independent vulnerability assessments was to identify and characterize major vulnerabilities of the tag/seal device during the development process, and hence, enable the developer to produce a better tag/seal technology. The "reader" device was never specifically assessed since it was always assumed to be under the inspecting signatory's control. INEL's principle objective in each assessment was the identification of one major vulnerability. A major vulnerability is an attack methodology which results in a tampered tag/seal that passes both a physical (i.e., visual and mechanical) inspection and provides statistically acceptable (compared to reference data) signature results.

After a major vulnerability was shown to exist, it along with any other unassessed potential

weakness areas would be presented to the technology developer. It was always assumed that the developer would resolve the major vulnerability, and then assess the other potential weaknesses for further design modification impacts. The modified tag/seal design would then be completely re-assessed.

No specific time limits were imposed on the implementation of any method of attack, but the shortest possible implementation time using the most simplistic approach was the major goal and a primary consideration in formulating attack methodologies. No attack methodology was considered if it could not be performed in the field or if its implementation was inconsistent with the specified tag/seal application environment. No cost ceiling was imposed on the fieldable hardware required to perform an attack; however, all attack methods used mostly low-cost and commonly-available tools.

4. Assessment Approach

The tag/seal technology developer provided multiple units of a specific tag/seal design, a complete technical description of the tag/seal device including its uniqueness and sealing properties, a prototype reader including its operation and signature acquisition and correlation method, and any reader interface for tag/seal signature acquisition. Each INEL assessment included three focus areas: an initial application assessment, a system operational performance study, and a tag/seal device analysis. The first two focus areas were very important in establishing the basis for selecting viable adversarial attacks.

3.1 Application Assessment

Many factor[2] are important in determining the applicability of a tag/seal technology to a given application. The following factors were used in INEL adversarial assessments:

- **Treaty-Limited Object:** The size and shape of the object(s) or container(s) to be tagged were important determinants of design requirements (such as length, flexibility, strength, visible and non-visible access for subsequent inspections, etc.) When the specific object was undefined, general applications, relative to current treaty negotiations, were assumed.

- **Effectiveness:** This was defined as the expected level of a deployed tag/seal's resistance to circumvention by such measures as counterfeiting and replacement or removal and resealing. Only the highest level of resistance was expected of each tag/seal technology.

- **Physical Environmental Exposure:** The effects of environmental exposure may help conceal certain attacks. Hence, an assessment was performed to determine the results of those effects, such as scratches, normal wear and tear, etc., which could affect the tag/seal appearance without degrading operational performance.

3.2 System Operational Performance Study

Operational performance of a tag/seal system defines the baseline for what is expected for any proposed vulnerability assessment. Two important issues affecting this baseline are:

- **Technology Performance and User Training:** A prototype system would be fully demonstrated and its performance objective described using multiple, assembled tag/seal devices. This system would then be made available for vulnerability assessments. These tag/seal devices and their corresponding signatures provided a database of reference signatures for assessing the effectiveness of an attack method.

- **Inspection Procedure and Acceptance Criteria:** When it was possible, the tag/seal technology developers provided inspection procedures and acceptance/rejection criteria for their technologies. However, the developmental status of the technologies usually precluded definitive statements of acceptance/rejection criteria. In these instances, INEL defined such criteria based on maintaining physical (as-assembled) appearance and on statistical similarities and differences in signature readings of the developer-supplied tag/seals.

3.3 Tag/Seal Device Analysis

Most of the effort in each adversarial analyses was directed to the analysis of the tag/seal device. The attack methodology varied depending on the specific tag/seal design and application, but a general analysis protocol was followed.

- **Component Analyses:** The mechanical, electrical, and chemical properties of the tag/seal component materials were characterized. While all material components were included, efforts were concentrated on those components associated with uniqueness determination and sealing effectiveness.

- **Weakness Identification:** Using the component analysis, the operational performance data, and the initial application assessment, any weaknesses in the design were identified.

- **Weakness Down-selection:** Weaknesses that appeared to be the most susceptible to attack were selected after initial laboratory experiments and fundamental weakness studies. These studies included such considerations as the attack time, hardware requirements to expose the weakness, the attacker's expected level of expertise, the number of attackers required, diagnostic instruments required, etc. In most cases, no more than three potential weakness areas could be identified for a technology. Applicable attack methods were identified for each of the down-selected weaknesses.

- **Vulnerability Analyses:** Using the most vulnerable weakness area, the corresponding

attack methods were implemented on a single tag/seal device. Based on the degree success, the attack was either repeated on additional tag/seal devices to assess repeatability and learning curve effects or another identified attack method was applied against that weakness area. This process was continued until an attack scenario was successful or until all selected weakness areas had been evaluated. Attack success or failure was determined by the related inspection procedure and its corresponding signature acceptance/rejection criteria. Any identified vulnerabilities were corrected in follow-on designs.

5. Integrated Vulnerability Assessment Concept

The integration of vulnerability assessment within a tag/seal development effort rather than performing vulnerability assessments on completed designs, can lead to much better end-products. The vulnerability assessment model within the DOE high-security tag/seal technology program may not be directly applicable to every tag/seal development effort, but it has shown itself to be highly effective. An integrated assessment concept can be cost-effectively applied throughout various stages of a developing technology and can lead to a high level of customer confidence in applying a successfully assessed tag/seal technology. Similar vulnerability assessments can be applied to selecting developed tag/seal devices for future applications, such as international safeguards and nuclear material controls.

6. Summary

The integration of continuous vulnerability assessments into the DOE tag/seals development program has been described. INEL's overall adversarial role and philosophy are described relative to this tag/seal development effort. The integrated vulnerability assessment approach is recommended as a viable and cost-effective method of enhancing overall tag/seal technologies and improving customer confidence in deploying a given tag/seal technology.

REFERENCES

1. Fuller, J., et al., "DOE's Tags and Seals Program," Verification Technologies, DOE Report DOE/DP/OAC/VT-92B, Oct. 1992, pp. 4-41.
2. "Tags and seals for controlling nuclear materials," Arms Control and Nonproliferation Technologies, DOE/AN/ACNT-93A, Second Quarter 1993, pp. 11-30.

DISCLAIMER