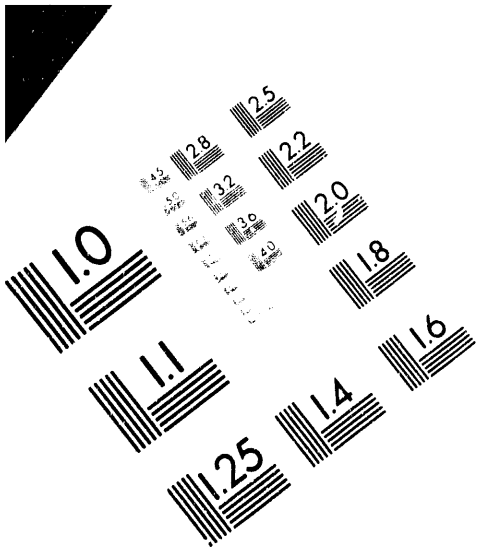
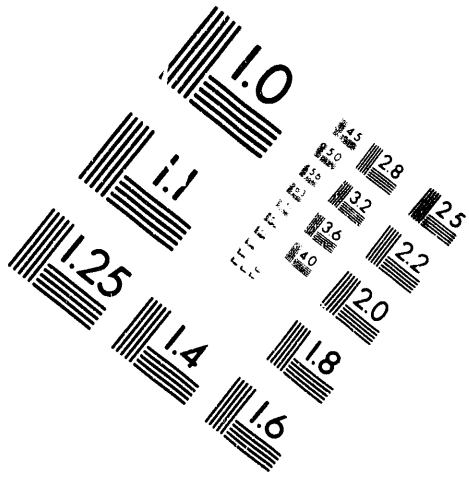
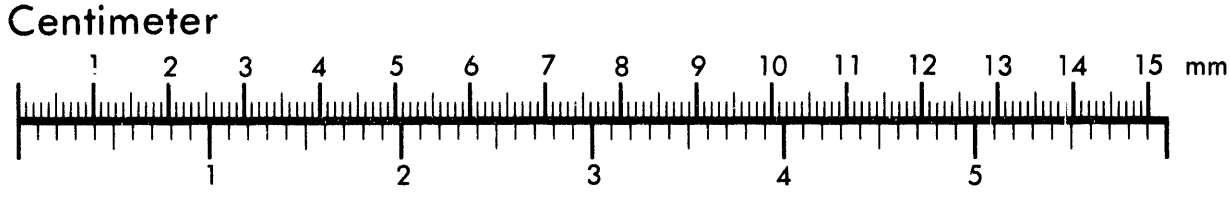


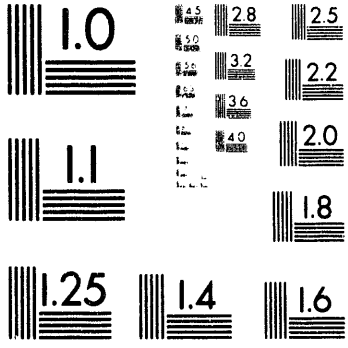
Association for Information and Image Management

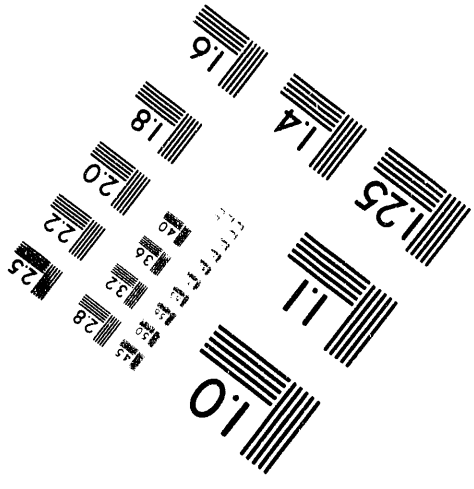
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

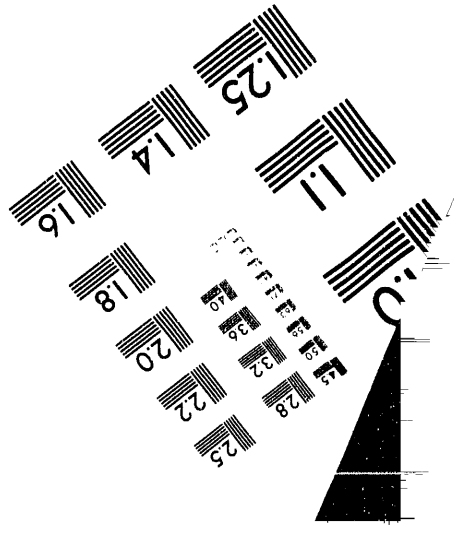
301/587-8202











1 of 1

Conf-930749--21

Passive Tamper-Indicating Secure Container

Jack C. Bartberger
Member of the Technical Staff
On-Site Monitoring Technology Department 9249
Sandia National Laboratories
Albuquerque, New Mexico
87185-5800

All papers must include the following statement:
This work performed at Sandia National Laboratories is supported by the U.S. Department of Energy under contract DE-AC04-76DP00789.

Abstract

This paper describes a *passive tamper-indicating secure container* that has been designed to demonstrate concepts, features, and materials that can be used in *passive* container applications. (In a passive security system, physical phenomena provide *visual* indication of tampering.) The basic container "volume within a volume" assembly consists of a transparent plastic outer container and an aluminum inner container. Both containers incorporate passive, fingerprinted layers as part of the tamper-indicating container system. Many of the tamper-indicating features can be visually inspected without disassembling the container. The status of container development and potential applications for the container are addressed.

Introduction

Solving the problem of protecting sensitive items stored in an unmonitored environment from undetected tampering is crucial to the success of a non-proliferation policy that must reliably monitor and verify critical activities. The items required to accomplish this could include process monitoring equipment, inspection equipment, or any items for which passive security measures could be used to provide an acceptable level of tamper-indication when the items are not in a protected, secured environment. The spectrum of adversarial tampering ranges from attempted concealment of "pin-hole" size penetration to complete container destruction that might involve counterfeiting or replacement efforts.

Tamper-indicating technologies that can be applied to containers are currently under development for both *passive* and *active* applications. *Passive* protection relies on physical phenomena to provide a visual indication of tampering when the protected item is inspected. *Active* protection involves the application of sensors of various types to monitor the protected volume and provide *electrical information* that indicates whether an unauthorized activity relative to the protected volume has occurred. Active security requires a power source to function as a tamper indicator, while passive security does not.

The term *tamper-indicating* refers to design features that produce physical evidence of unauthorized access. In a *passive* security container system, the tamper-indicating features would be visible, and non-repairable or non-replaceable features could be used to verify the integrity of the container assembly.

Passive Tamper Indication

Sandia National Laboratories has been funded by the Defense Nuclear Agency (DNA) to provide technologies that can be applied to a *passive tamper-indicating secure container.* The current design is based on a "layered" concept of passive tamper indication. The security provided by this design results from the number of passive tamper-indicating layers and the features incorporated into these layers that an adversary would have to defeat the protected volume.

The container described in this paper has not been designed for a specific application, but rather is a generic product that can be used to demonstrate passive concepts, features, and materials related to tamper-indication. It provides the opportunity to investigate the synergistic effects of various tamper-indicating features in a cost-effective manner. The design criteria have been considered both from the vulnerability and inspectability aspects, as well as for manufacturability and cost. Therefore, the lessons learned from this particular design are applicable to future projects that might benefit from the passive tamper-indicating features and materials incorporated into the container.

Design Criteria

The design criteria and design goals required to develop the *passive tamper-indicating secure container* concept are listed below. (They are not listed in order of significance.)

1. The exterior container must be transparent to permit visual inspection of the interior container.
2. The exterior container should be plastic to provide the transparency feature.
3. The exterior container should have minimal visual discontinuities to discourage an adversary from attempting to tamper with or penetrate the container itself.

ds

4. The exterior container should be designed to be permanently assembled; disassembly should not be possible without some obvious form of destruction.

5. The exterior container should incorporate tamper-indicating and tamper-resistant features that would result in visible damage that is readily apparent to an inspector, while being extremely difficult for an adversary to repair. These features should not provide an adversary with a point of attack that would be advantageous to the concealment of a tamper attempt.

6. The inside surfaces of the exterior plastic container should have a passive coating(s) that provides additional visible tamper indication.

7. The plastic parts should be molded from ultraviolet (UV) stabilized polycarbonate to enhance the durability of the container in outdoor sunlight conditions.

8. The interior container should not be transparent, and therefore should not be made from a plastic material. This would require that a different material be used than the material used for the exterior container, requiring an adversary to develop another attack technique.

9. The mounting features and outside surfaces of the interior container should be visually inspectable. The mounting features should be as simple as possible.

10. The interior container should have a passive tamper-indicating coating(s) on its surfaces (inside and/or outside).

11. Any coating(s) used on either the plastic or metallic container should be capable of incorporating a unique fingerprint feature for identification purposes.

12. The design must be compatible with any coating technologies that are appropriate for passive tamper indication.

13. The plastic parts should be inexpensive, cost-effective, and disposable since authorized access to the contents in the interior container will require the destruction of the external plastic container.

14. Materials required for the various tamper-indicating features must be environmentally safe and present minimal hazards in both their application and disposal.

15. The fabrication of the various components required for the container must use "off-the-shelf" technologies; i.e., injection molding and commercially available metallic containers.

Container System Overview

The basic design concept for the passive secure container system is a "volume within a volume," incorporating passive tamper-indicating and tamper-resistant features on both interior and exterior volumes, or containers (Figure 1). Many of these features can be visually inspected without disassembly because the exterior container is transparent polycarbonate plastic and the interior container is aluminum.

The exterior container has been designed for one-way assembly — it cannot be removed or opened without being destroyed. Therefore, access to the interior volume requires destruction or penetration of the outer plastic container and the subsequent destruction or penetration of its internal tamper-indicating layer(s). To conceal tampering, an adversary would have to repair or replace anything (components, coatings, materials, etc.) that could indicate that tampering has occurred. The design goal is to make it difficult for an adversary to gain undetected access to the contents of the interior container and to make it difficult to conceal any attempt at unauthorized activity.

Passive tamper-indicating coatings for the interior surfaces of the transparent plastic exterior container are currently being investigated. These include, but are not restricted to, transparent UV-cured materials and clear silicones. A passive tamper-indicating coating for the

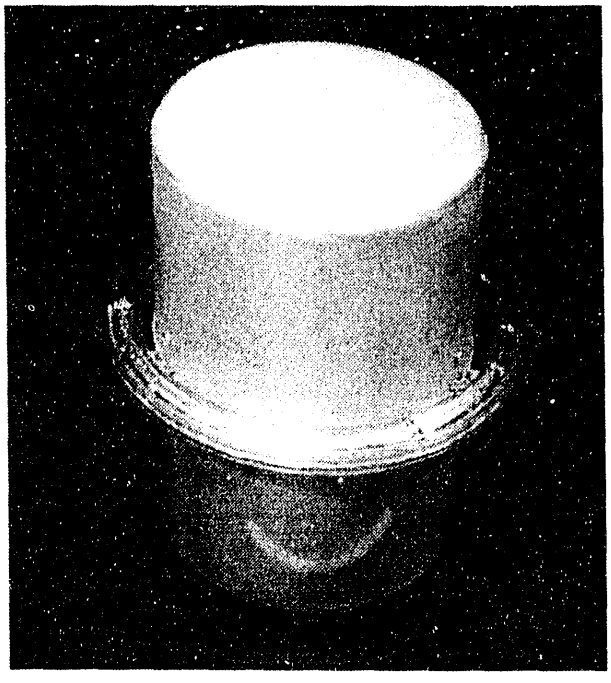


Figure 1. Assembled Tamper-Indicating Container

aluminum container is the result of a fluorescent anodize process and is currently under development. In addition, the coatings for both the interior and exterior containers have unique and random fingerprint features associated with them. This additional feature prevents substitution of a counterfeit container by an adversary.

The interior and exterior containers are separated by about 1/2 inch of space all around, except for three small mounting features that support the aluminum container within the confines of the plastic container. The resulting effect is that the interior container appears to be "suspended" within the exterior container. All outer surfaces of the aluminum container and the associated mounting hardware are visible for inspection, but are not physically accessible unless the plastic container is penetrated or removed. Tamper-resistant hardware is used to mount the metallic interior container within the plastic exterior container. The plastic container is not reusable since access to the interior volume requires its destruction or penetration. However, the aluminum container can be reused.

Hardware Description

Mechanical Design of the External Container

The items required to construct the external polycarbonate container consist of two identical *housings* and one *flange* (Figure 2). Injection mold tooling has been fabricated to produce the plastic parts, which have been molded by a commercial injection molder in quantities sufficient to characterize the molding process (temperatures, cycle time, injection shot size, mold packing, tooling functionality, etc.). The external plastic container is designed for *one-way assembly*: commercial push-on type "self-locking" fasteners are used to mechanically assemble the plastic container components together. The assembly is permanent, and the components cannot be separated unless the fasteners are defeated or destroyed or the outer plastic container components are broken or cut in some manner.

The fasteners and the associated mechanical features of the plastic parts are designed and located to permit visual inspection for tampering from outside the assembled container. In addition, the flange component provides mounting features for the internal container.

The plastic housing has both male and female features (6 each) on the interface surface that, in conjunction with the push-on-fasteners and the plastic flange, provide the method of permanent assembly. Only when these features are oriented properly with respect to each other on opposite sides of the flange, i.e., male to female, as shown in Figure 3, can the container be assembled.

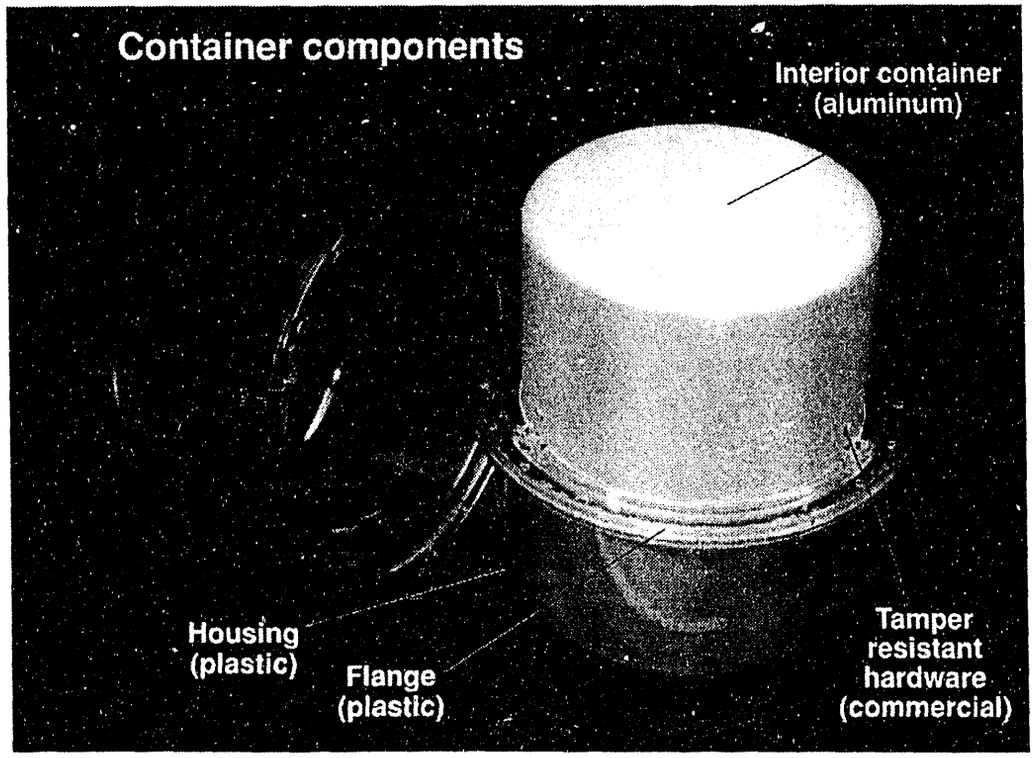


Figure 2. Tamper-Indicating Container Components (pre-assembly)

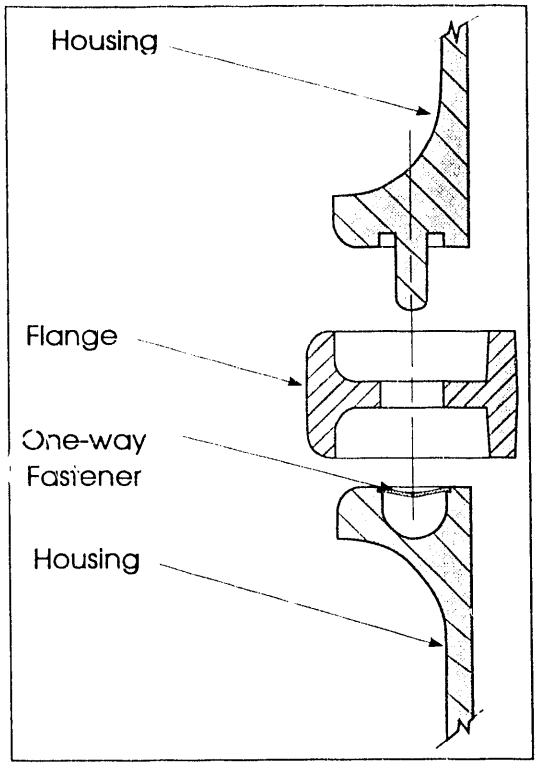


Figure 3. Flange and Housing

A Clamp Ring Assembly Tool has been fabricated to press the plastic container assembly together. The six fasteners are retained at the female locations of each housing with silicone adhesive.

The result of the assembly operation is that each housing is fastened to the flange, in six places, by the fastener that is co-located on the opposite side of the flange. The fasteners are captive between the flange and the respective housing and cannot be removed. A total of 12 fasteners that simultaneously secure both housings to the flange provide the permanent one-way assembly feature.

Tamper-Indicating Features of the External Container

The mechanical and physical features of the plastic parts have been designed to provide maximum visual access for inspection of the assembled container, especially in the fastening areas where the flange and housings interconnect. As a result, the plastic features, such as the fastening areas and the fasteners themselves, are subject to a certain degree of inspection. As previously stated, the ability to inspect the container features was determined to be important to the basic concept of visual indication of tampering. Also, visual discontinuities have been kept to a minimum because they are advantageous to an adversary. Disguising a tamper attempt and its repair should not be made easier by the optical or physical characteristics of the injection-molded parts.

Both the limitations and the advantages of features resulting from the injection-molding process have been assessed, and their resulting effects have been considered during the concept and design stages for the plastic components. For example, the requirement for injection-molded parts to have a draft angle, or taper, for removal from the mold has been used whenever possible to enhance tamper-resistance. Cutting tapered features with a saw blade (or similar tool) removes material, commonly referred to as the "kerf."

Visual discontinuities also can offer an adversary a point of attack that allows tampering to be concealed. Such visual discontinuities occur when sharp edges and corners are formed in plastic, and would be particularly noticeable in transparent parts such as the housing and flange. A radius has been designed into the features of these components, wherever appropriate, in order to eliminate this visual characteristic. Like the taper, the radius is difficult to repair in a manner that conceals the effects of tampering.

A labyrinth joint arrangement has been used at the interface between the housing(s) and the flange. Once the plastic container has been assembled, there are no "straight-through" penetration points or areas that provide obvious access to the interior volume. Consideration also was given to minimizing the visual and mechanical aspects of this area that might provide vulnerabilities or features that could conceal tampering and not be visually inspectable.

In addition, tamper-indication on the plastic container can be enhanced by installing a coating on the internal surfaces of the container, requiring an adversary to contend with this added layer of protection in order to conceal any evidence of tampering. The coating makes both penetration and restoration more difficult. Some polymeric coatings currently being evaluated at SNL include (1) epoxies, (2) silicones, (3) polyurethanes, (4) polyesters, and (5) acrylic resins. All these coatings are commercially available. Attempts to penetrate the container would result in a visible delamination of the coating on the inside surfaces of the container, creating a bubble or tear in the coating. Once the delamination occurs, it would be difficult or impossible to repair without access to the inside of the container. Materials that produce this coating (normal air-dried or heat-cured systems, as well as the faster curing UV formulations) are currently being evaluated for their application methods, appearance, and delamination characteristics.

The coatings will be applied to all of the interior surfaces of the plastic container. Although they may have some tint associated with them, depending on the characteristics of the particular coating material, they are basically transparent. They may also have additional fingerprinting or tamper-indicating additives that would not necessarily be transparent. These additives would provide a unique and random pattern that could not easily be reproduced and could be documented for later verification and anti-counterfeiting purposes. Some examples of the additives include fluorescent dyes or particles, coloring agents, glass micro-balloons, and organic or inorganic particles, such as glitter or hematite. Because the outer container is transparent, some of the coatings could contain features that would be visually inspectable from outside the container assembly. However, there may be other features that would only be inspectable from the inside and would not be evident until the container has been cut open, as described below.

Once the container has been opened, the inspector would have the option of performing a detailed *post-mortem* inspection, in a laboratory environment, to verify the authenticity and integrity of the container system based on the unique fingerprint features. The *post-mortem* inspections could be done from a physical viewpoint (essentially, from inside looking out).

Opening the External Container

The sequence for opening the secure container for *post-mortem* inspection is relatively simple — cut the exterior plastic container open to gain access to the interior container for inspection of its tamper-indicating features and hardware. A commercial, battery-powered circular saw has been modified to provide a simple method of cutting the polycarbonate material. It takes less than 3 minutes to saw completely around the plastic container diameter. A small wooden stand also has been built to hold the container assembly during cutting for safety and convenience. The container can be cut open at any location between the flange and the three fasteners on the internal container for access to the tamper-resistant fasteners and subsequent opening of the internal container. After the plastic container is removed, a detailed inspection of the internal metal container can be performed to verify its authenticity. The interior container and its security features are described in detail below.

Because there are no obvious features to indicate where or how a container will be opened for *post-mortem* inspection, an adversary cannot use them to conceal any tampering or repairs. In fact, the plastic container may be opened by cutting at *any* location that is appropriate for access to the mechanical fasteners associated with the aluminum internal container.

Once the plastic container has been cut open, any interior layers (coatings, etc.) applied to it with fingerprint characteristics not previously visible from outside the assembly can be inspected. These could include coatings (or additives to the coating) that are UV sensitive. Because of the UV absorption characteristic of the plastic container itself, such UV sensitive characteristics cannot be inspected until the container has been opened. Documentation of the unique fingerprint features, such as Polaroid, 35mm photography, or video, would be required for the *post-mortem* inspection to verify that the coating is the original and has not been tampered with or replaced.

Mechanical Design of the Internal Container

The internal metal container is constructed from two commercially fabricated, deep-drawn aluminum housings that have been modified for mounting to the flange component of the outer container (Figure 2). These are stock items made from type 3003-0 aluminum. One of the housings has been flared at the open end to a depth of approximately 0.250 inch to create an overlap, and relatively snug fit, when the aluminum housings are mounted together to the flange. This creates a mechanical feature (labyrinth) that adds to the tamper resistance of the design. A special anodizing process applied to the surfaces of the aluminum provides a random fingerprint feature and tamper-indicating layer on the interior container. This process can be applied to both outside and inside surfaces of the aluminum parts.

The aluminum housings are both fastened to the flange by means of three simple aluminum angle brackets at each of the three spokes of the flange. The brackets are inside the metal containers for functional and aesthetic reasons. Several types of commercial "tamper-proof" or "tamper-resistant" hardware are used for mounting the aluminum containers to the brackets. This type of hardware requires special tools for removal (and installation), and thus can provide some additional deterrence to an adversary. After the container is assembled, the screw heads are visible for inspection from outside the plastic container. Various combinations of the tamper-resistant hardware could be used as appropriate. Once the container system has been assembled, this hardware cannot be accessed without destroying or penetrating the outer plastic container.

One goal of the design concept was to have an absolute minimum number of mounting features that would impede visual inspection of the interior volume, yet still

provide a rigid mechanical assembly. The result of this design is a "volume that is suspended within another volume," except for the mounting features required for the interior container. The inspector can visually inspect the entire external surface of the aluminum container from outside the plastic container. Thus, avenues that an adversary could use for undetected penetration of the interior volume are minimized.

The flange requires some minor modifications (secondary machining) after injection molding to accommodate mounting the interior volume. Essentially, after modification, there are three plastic "fingers" (approximately 0.125-inch thick by 0.250-inch wide) of the flange spokes that protrude through three corresponding notches in the aluminum container at the interface joint. The spokes are modified only at the interface locations where they protrude through the aluminum. This provides maximum integrity of the interior volume by minimizing the number and size of penetrations through it. The remaining portions of the spokes (inside the aluminum housing) are unmodified and are available for mounting any items that the container may be used to protect. The structural integrity of the flange is unaffected by the modifications described.

The flange has been designed to be as versatile as possible to accommodate potential applications. The mounting configuration for the secure container described in this paper is only one of numerous possibilities. Different configurations could be used depending on the application. It should be noted that the spokes could be entirely removed from the interior container area and the angle brackets redesigned to provide an unobstructed volume within the aluminum container if that is required.

Tamper-Indication and Unique Fingerprints for the Internal Container

The internal aluminum container also has tamper-indicating features associated with it in the form of various post-anodize treatments that enhance the inherent characteristics of an anodized surface. These can include fluorescent additives and unique fingerprint patterns, both random and structured, that would be visible for inspection under certain conditions, i.e., only after removal of the plastic container and with exposure of the metal container to a source of UV light. These additives and the associated pattern created are sensitive to UV light. Thus, the aluminum housing is a fingerprinted, one-of-a-kind item that is believed to be very resistant to the typical tamper/ repair scenario associated with anodized surfaces.

Because the outer container is injection molded from UV-stabilized polycarbonate, it does not pass light in the UV portion of the spectrum. For the secure container, however, this UV stabilization factor adds a unique capability that complements the tamper-resistant features of the anodized aluminum. The assembled container system does not provide an adversary visual access to the fluorescent fingerprint feature because of the UV stabilization of the plastic container and consequently presents the adversary with an unknown layer of tamper-indication. The unique and non-reproducible fingerprint features will require documentation in order to allow subsequent verification of container authenticity. This documentation could be a photographic record of some type, such as Polaroid, 35mm photography, or video.

Status and Future Development

The *Passive Tamper-Indicating Secure Container* is in its second year of development. Efforts to identify and apply coatings with tamper-indicating features are ongoing. The project is scheduled for completion in December 1993. The container hardware and the associated coatings will be subjected to in-house vulnerability assessments and evaluations by Sandia experts throughout the project life cycle. Design improvements will be incorporated as appropriate based on schedules and funding considerations.

A container application study will be initiated by mid-1993 for the protection of a commercial video camera and associated electronics for data collection in an unmonitored environment. A limited hardware demonstration of the concept is planned.

Summary

The *Passive Tamper-Indicating Secure Container* is generically designed to address the problem of volume protection in a cost-effective manner by using existing technologies and materials to produce a multi-layered security container. Its primary function has been to provide a vehicle for the development of these tamper-indicating coatings and tamper-resistant features. The ultimate goal is to use the concepts and technologies developed with this container system for specific applications that require cost-effective, *passive* tamper-indication for equipment during storage and transportation.

DISCLAIMER

DATE
FILMED
9/21/93

END