LA-UR-96-3672

Title: **Vulnerability Assessment of Security Seals**

Author(s): R.G. Johnston

Submitted to:

http://lib-www.lanl.gov/la-pubs/00418796.pdf

Los Alamos
NATIONAL LABORATORY

Form No. 836 R5
ST 2629 10/91

LAUR #96-3672

Vulnerability Assessment of Security Seals

Roger G. Johnston, Ph.D. and Anthony R.E. Garcia
Los Alamos National Laboratory

Abstract

Tamper-indicating devices, also called security seals, are widely used to detect tampering or unauthorized entry. We studied 94 different security seals, both passive and electronic, developed either commercially or by the United States Government. Most of these seals are in wide-spread use, including for critical applications. We learned how to defeat all 94 seals using rapid, inexpensive, low-tech methods. Cost was not a good predictor of seal security. It appears to us that many of these seals can be dramatically improved with minor, low-cost modifications to either the seal or the use protocol.

Introduction

Tamper-indicating devices, also called security seals, are widely used in industry and government (Kissane and DeSanto, 1992; Rosette, 1992; ASTM, 1988 & 1990; Staehle, 1992; NRC, 1996). Seals are not locks--they are not intended to stop unauthorized access. Seals are instead meant to leave unambiguous, non-erasable evidence of entry or tampering. Applications include access control, records integrity, inventory, shipping control, theft prevention/detection, hazardous materials accountability, nuclear nonproliferation, national defense, law enforcement, customs, counter-terrorism, counter-espionage, protecting instrument calibration, securing surveillance/monitoring equipment, and protecting consumer products.

Seals take a variety of forms (Staehle, 1992; ASTM, 1988 & 1990; Rosette, 1992; Gritton and Riley, 1992; Horton and Waddoups, 1995; NRC, 1996). Examples include frangible films or pressure sensitive adhesive tapes, crimped cables or other (supposedly) irreversible mechanical assemblies, security containers or enclosures that give evidence of being opened, devices or materials that are intended to display irreversible damage or changes when manipulated, and electronic systems that continuously monitor for changes such as a break in an electrical cable or fiber optic bundle.

We have previously (Johnston et al., 1995; Johnston, 1996) reported on a vulnerability assessment of 79 different passive, i.e., non-electronic, seals, many in use or under consideration for nuclear applications. The present paper incorporates these findings, as well as additional results on the original 79 passive seals, and new analyses of 15 other seals, including electronic ones. The 94 total seals we have now analyzed include both commercial and government-developed devices. Many are in wide-spread use by government or industry for both routine and critical applications. Table 1 shows the type of seals that we have assessed.

It is not our intent in this paper to single out specific products for comment, nor to disseminate information on how to defeat security seals. We instead want to emphasize generic findings and share some of the lessons suggested by our work.

Terminology

A comprehensive "vulnerability assessment" of a seal, in our view, involves the following goals:

1. Establish the appropriateness and effectiveness of the seal for a given application.
2. Identify its strengths, weaknesses, and vulnerability to attack.
3. Attempt to find counter-measures for any identified vulnerabilities. These may include application-dependent or independent methods of improving the security of the seal, either by modifying the seal itself or by improving the procurement, installation, inspection, removal, or disposal procedures.

The findings presented in this paper concern mostly goal #2.

"Passive" seals are defined as tamper-indicating devices that use no electrical power (internal or external) when in use. Some passive seals are designed to be examined or interrogated at inspection time using an electronic instrument, but they are still considered passive if non-electrified most of the time.

In this paper, the term "attack" shall refer to an attempt to avoid detection while gaining entry through a seal to whatever the seal is protecting. A successful attack (one that is not detected) is also referred to as a "defeat".

Defeating a seal consists of opening the seal without any detected damage or evidence of entry; or opening the seal and repairing any damage and/or erasing detectable evidence of entry; or replacing the entire seal with a counterfeit that will be confused with the original; or replacing relevant parts with counterfeits. This general description of possible seal defeats is somewhat broader than that offered by ASTM Standard F1158-88 (ASTM, 1988) or British Standard BS 7480:1992 (BSB, 1992).

The emphasis in our work is on "low-tech" attacks. We define a low-tech attack as one that uses relatively low cost tools and supplies readily available to the general public, at least in small quantities. A low-tech attack may exploit access to a conventional home or commercial machine shop. It may also utilize assistance or information readily provided to anyone by the seal manufacturer or user. An attack can still be considered low-tech even if, to be successful, it requires considerable practice and/or skill with the hands at the level of an average artist or artisan.

In discussing vulnerability assessments with seal developers, manufacturers, and users, we have found it useful to categorize the thoroughness of a defeat. Towards this end, we have developed the Los Alamos Seal Defeat Categorization Scheme. We classify defeats at type 1, 2a, 2b, or 3. This is a slight modification to our original classification scheme that involved types 1, 2, and 3 (Johnston et al., 1995).

In a type 1 defeat, tampering is not detected if the "usual" seal inspection process is followed. The usual process is that routinely or typically employed by the end-user. For most seals, this is the protocol recommended by the developer or manufacturer of the seal. A type 1 defeat, however, will be detected if unusual efforts are taken. For many seals, an example of an unusual inspection protocol would be to disassemble the seal and examined it in great detail to look for tampering.

In a type 2a defeat, tampering is not detected if the usual inspection protocol is followed and if the user visually studies the exterior of the seal (plus any internal parts that can be seen without opening the seal) to look for evidence of entry. The visual inspection can be done with either the naked eye or a hand-held magnifier.

In a type 2b defeat, tampering is not detected if the usual inspection protocol is followed and if the user disassembles the seal and meticulously examines the interior and the exterior of the seal visually (with the naked eye or a hand-held magnifier) to look for evidence of entry.

In a type 3 defeat (the most thorough), tampering cannot be detected, even if the most advanced postmortem analysis is undertaken. State-of-the-art techniques in forensics, material science, or microscopy will not be able to tell that the seal has been defeated.
If a non-type 3 defeat is successful in a seal application where the "usual" inspection protocol automatically includes meticulous visual examination of the exterior or interior of the seal, the defeat is classified as 2a or 2b, respectively, rather than as a type 1 defeat.

Results

We devised and demonstrated 1, 2, or 3 different defeats for each of the 94 seals we analyzed, for a total of 132 defeats. Table 2 shows a classification of the defeats into types 1, 2a, 2b, or 3.

All 132 defeats were low-tech. For most of the seals, we have devised, but not yet fully demonstrated, additional low-tech attacks. Attacks using high technology are probably also possible, but are not necessary to defeat any of the 94 seals we examined.

All of the 132 defeats we demonstrated can be implemented with tools and supplies that can be carried easily by one person. In some cases, all necessary tools and supplies can be concealed in one hand or in a pants pocket.

With practice, the time to successfully complete the attacks varied from 3 seconds for several of the seals to 125 minutes for the most difficult. Figure 1 shows the histogram of defeat times for the demonstrated defeats. The mean time to complete the 132 defeats was 4.3 minutes, with a standard deviation of 12.8 minutes. These defeat times are the time for one well-practiced individual to successfully complete the attack without assistance. For some of the attacks, the defeat time would probably be shortened if an assistant were available to help.

We found little correlation between the defeat time and the unit cost of the seal. The linear correlation coefficient was only $r=0.08$. The correlation is so weak that, on average, increasing the unit cost of a seal by $1 adds less than 1 second to the defeat time. For seals under $1 per unit (in quantities of 1000), there is no difference, on average, in the defeat time for more expensive seals vs. cheaper ones.

Figure 2 shows that there is also little correlation between the defeat time and the type of defeat (1, 2a, 2b, or 3). In fact, the more thorough type 3 defeats actually required less time on average than the type 1 defeats: 2.9 minutes vs. 5.3 minutes, respectively.
Figure 3 shows the defeat time for the various types of seals.

The low-tech nature of the attacks is emphasized in figure 4, where the cost of each successful attack is plotted vs. the defeat time. The cost of the 132 defeats was quite modest, ranging from $0.15 to $750, with an mean cost of $56.

The cost for each defeat is an estimate for all the equipment, tools, supplies, and services (e.g., machining in a commercial machine shop) needed to defeat one seal. If consumable supplies were needed for a given attack, the cost of purchasing the minimum commercial quantity is included in the cost estimate, rather than a pro rata estimate of the amount of the supply actually used in the attack. Note that the marginal cost for each defeat, that is the cost to defeat a second seal using the same attack scenario, is substantially less than the cost estimates used to create figure 4. This is because many of the equipment, tools, and supplies involved in an attack can be reused.

The correlation between cost and defeat time in figure 3 is fairly strong, r=0.60. On average, each extra minute required to complete a defeat is accompanied by a $5 increase in the cost of the attack.

Concluding Remarks

There are some serious limitations and problems associated with this work (Johnston et al., 1995; Johnston, 1996). First of all, seals are but one aspect of most security programs. Defeating a seal in isolation of the complete program may not always be relevant. Ideally, vulnerability studies should evaluate seals in the specific, real-world context in which they are used. In this work, however, we developed attacks in terms of an actual application for only 9 of the 94 seals we studied.

Another potential problem with this work is the classification of the attacks. Classifying an attack as successful and of what type (1, 2a, 2b, or 3) was solely our own judgement for 24 of the attacks. Of the remaining attacks, 70 were discussed with independent seal or security experts, usually outside Los Alamos National Laboratory. An additional 22 were demonstrated to them. For 7 of the attacks, we provided samples of the defeated seals for informal examination. In all cases (discussion, demonstration, or provided samples), the experts agreed with our assessment that the attack was successful and of what type, 1, 2a, 2b, or 3.

Only for 3 of the 132 attacks did we do a rigorous double blind test. We had security personnel familiar with the seal try to determine which samples had been defeated. We did a blind test on 6 additional attacks. In these 9 cases, the security personnel were unable to detect which seals had been defeated, at the appropriate level of inspection (type 1, 2a, 2b, or 3). (In a double blind test, the seals are independently coded so that neither the experimenter nor the test subjects are aware of which seals have been defeated until after the test is completed. In a blind test, only the experimenters are aware of which seals have been defeated.)

The reasons for so few rigorous blind and double blind evaluations of our attacks include limitations on time and funding, difficulty in arranging realistic tests, and uncertainties about the context and real-world applications for the seals. Ideally, double blind tests of vulnerability should be conducted on security personnel unaware that a test is taking place. To ask security personnel which seal has been defeated is not a realistic way to evaluate real-world vulnerability. Adversaries do not usually announce to security personnel that they have defeated some of their seals. Tests on unaware security personnel, however, tend to be expensive, time-consuming, and difficult to arrange.
In analyzing this work, it is also appropriate to bear in mind that classifying an attack as type 3 is problematic. It is difficult to prove that no technology exists to detect a given attack. Neither we nor the independent experts who are aware of our work have envisioned any method of detecting our type 3 attacks, but that does not guarantee that such a method does not or will not exist.

With the above caveats in mind, this study presents several surprising findings. All 94 seals we studied can be defeated quickly and inexpensively using low tech methods and highly portable (sometimes concealable) tools and supplies. It is also surprising that there appears to be little correlation between defeat time and cost. One would expect the more expensive seals to be less vulnerable to attack. It was also unexpected that type 3 defeats (the most thorough) took less time on average than type 1. The reason for this may be that type 3 attacks, unlike type 1, cannot utilize cosmetic coverups to hide the attack. Such coverups are often quite time consuming.

Only 9 of the 132 defeats developed in this study involved substantial counterfeiting, that is, removing the original seal, then replacing it with a counterfeited duplicate. Counterfeiting, nevertheless, appears to be relatively simple for most of the seals. Manufacturers frequently make counterfeiting easier by providing free samples of the seals to anyone who asks; by using readily available materials or components; by using easily replicated colors, logos, or numbering; and by using such shallow embossing or stamping for logos or numbers that they can be easily buffed off and replaced with an alternative embossing or impression.

For most of our defeats, we believe that minor modifications to the seal would substantially increase the difficulty of an attack. These modifications would usually add little to the cost. Most seals would also benefit significantly from changes in the manufacturer's or user's protocol for procurement, storage, installation, inspection, removal, and disposal. Most of the changes we would suggest are relatively minor. For many seals, we believe that having security personnel aware of the most likely attack scenarios, and watching for them, would dramatically improve tamper detection. Seal users and manufacturers with a legitimate interest in tamper detection are welcome to contact us to discuss vulnerability issues.

Acknowledgments

This work was performed under the auspices of the United States Department of Energy. W. Kevin Grace and George Eccleston provided useful input.

References

American Society for Testing of Materials (1988). Standard Guide for Inspection and Evaluation of Tampering of Security Seals, ASTM Standard F1158-88, Washington, DC: ASTM.

American Society for Testing of Materials (1990). Standard Practice for Classifying the Relative Performance of the Physical Properties of Security Seals, ASTM Standard F1157-90, Washington, DC: ASTM.

British Standards Board (1992). Specifications for Security seals, British Standard BS 7480:1992, London, England: BSB.

Gritton, D. and Riley, M. (1992). Electronic Identification Devices. Energy & Technology Review, LLNL Report UCRL-52000-92. Livermore, CA: Lawrence Livermore National Laboratory.

Horton, Patrick R.V. and Waddoups, I.G. (1995). Tamper-Indicating Devices and Safeguards Seals Evaluation Test Report, Report SAND93-1726/2. Albuquerque, NM: Sandia National Laboratories Report.

Johnston, Roger G., Garcia, Anthony R.E., and Grace, W. Kevin (1995). Vulnerability Assessment of Passive Tamper-Indicating Seals. Journal of Nuclear Materials Management. [Vol.] 224, (1); 24-29.

Johnston, Roger G. (1996). Vulnerability Assessment of Commercial and Government Tags and Seals. Proceedings of the ASIS/DoD Security Seals and Tamper Indicating Device Symposium, Santa Barbara, California, USA, (February 6-7, 1996), pp. 25-36 and 55-71.

Kissane, C.P. and DeSanto, J. (1992). Cargo Theft Loss Prevention Techniques. In L.J. Fennelly (ed.) Handbook of Loss Prevention and Crime Prevention. Boston, MA: Butterworth.

Rosette, Jack L., (1992). Improving Tamper-Evident Packaging. Lancaster, PA: Technomic Publishing.

Staehle, G. (1992). DOE's Tags and Seals Program. Verification Technologies, DOE Report DOE/DP/OAC/VT-92B. Washington, D.C.: U.S. Department of Energy Report

U.S. Nuclear Regulatory Commission (January, 1996). Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material, Draft Regulatory Guide DG-5005. Washington, DC: U.S. Nuclear Regulatory Commission.

Table 1 - Types of Seals Assessed

seal type	number of different designs
adhesive tape	28
plastic	13
wire loop	8
metal cable	18
metal ribbon	10
bolt type	10
secure container	2
passive fiber optic	2
electronic	3

Table 2 - Categorization of the 132 Defeats

Los Alamos Defeat Category	number of demonstrated defeats
Type 1	26
Type 2a	60
Type 2b	23
Type 3	23

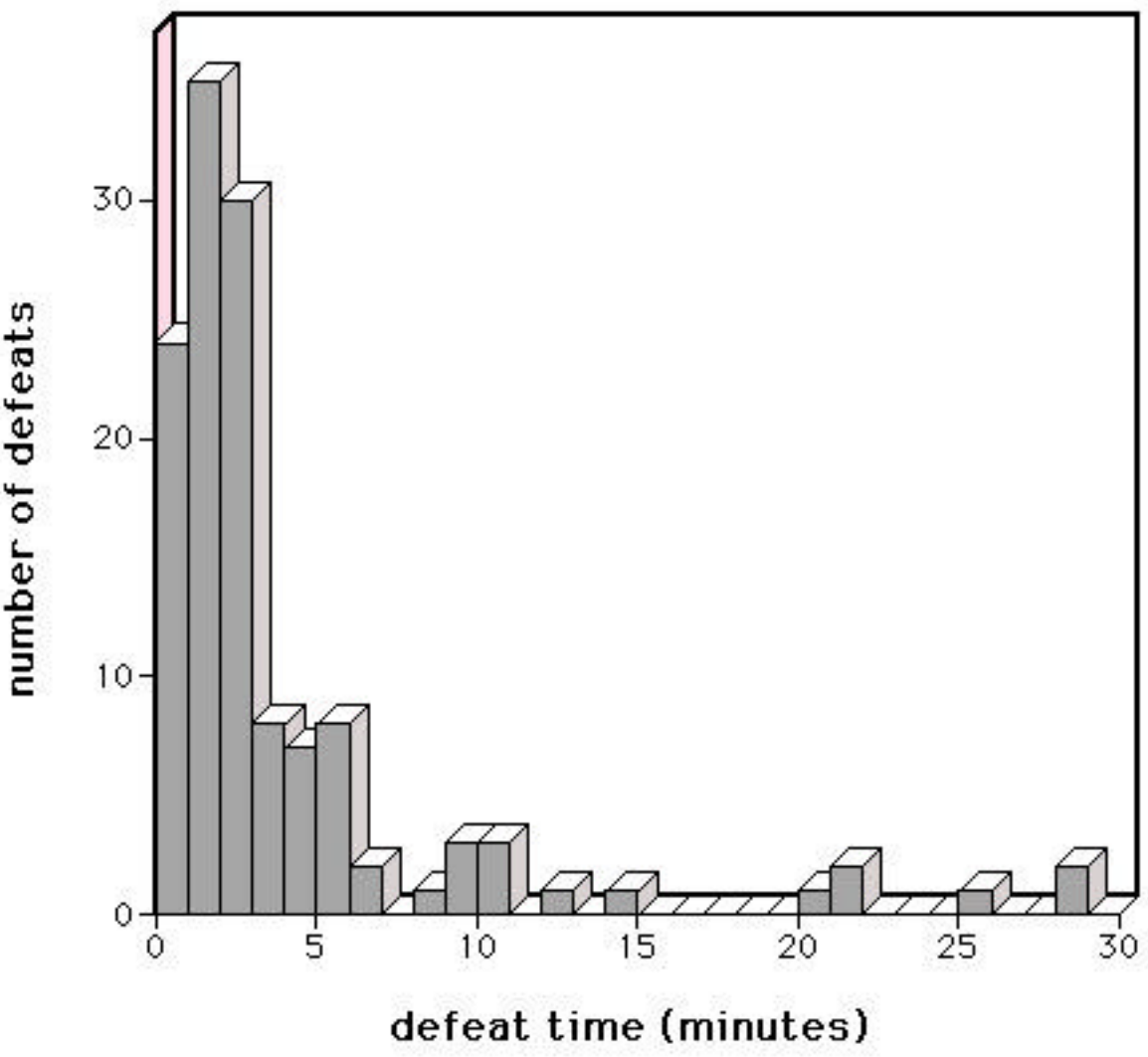

Figure 1 - Histogram of Defeat Times. This shows the time to defeat a seal (with practice) for our 132 attack scenarios. Two defeats are off scale at 45 and 125 minutes.

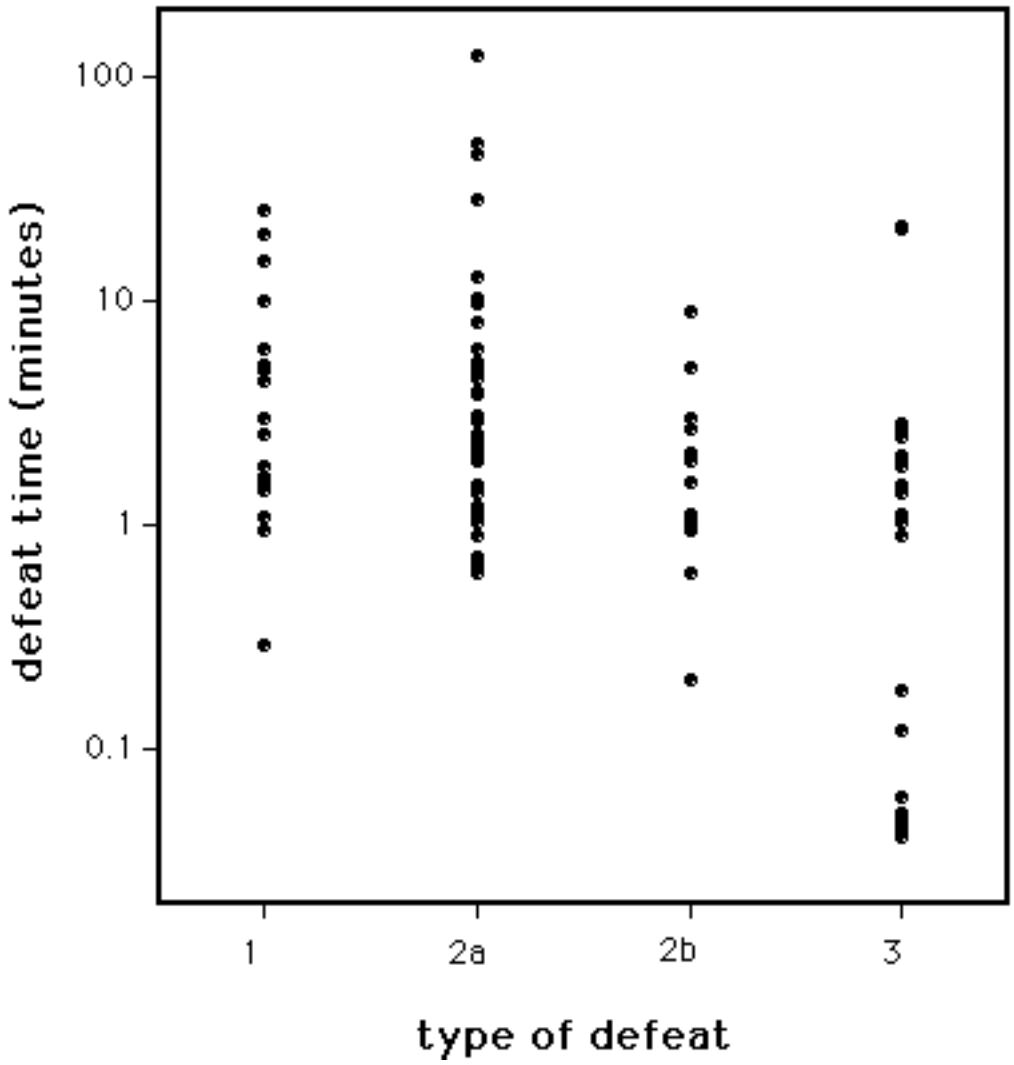

Figure 2 - Defeat Time Versus the Type of Defeat.
A total of 132 different defeats are shown in this scatter plot.

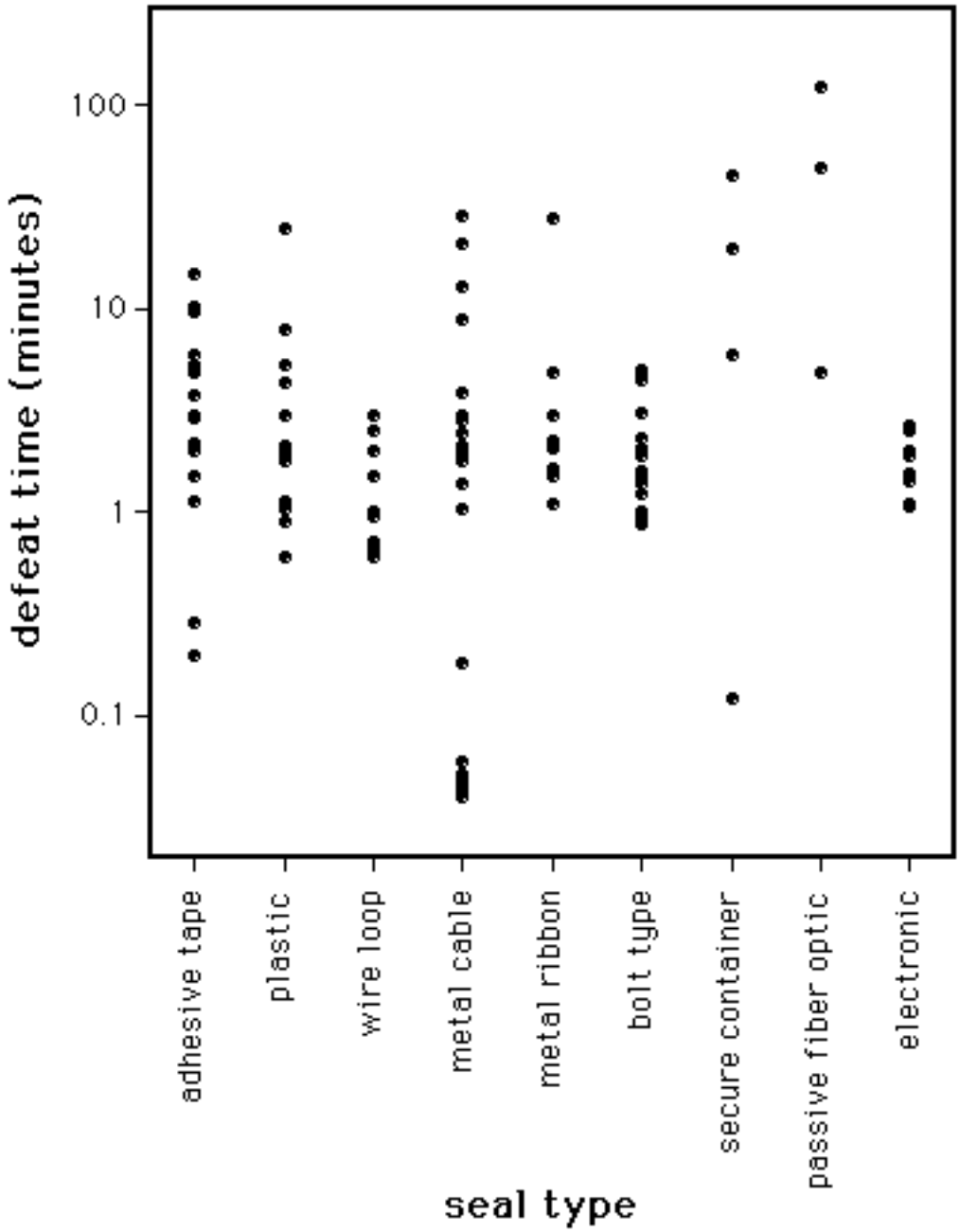

Figure 3 - Time to Defeat a Seal Versus the Type of Seal.

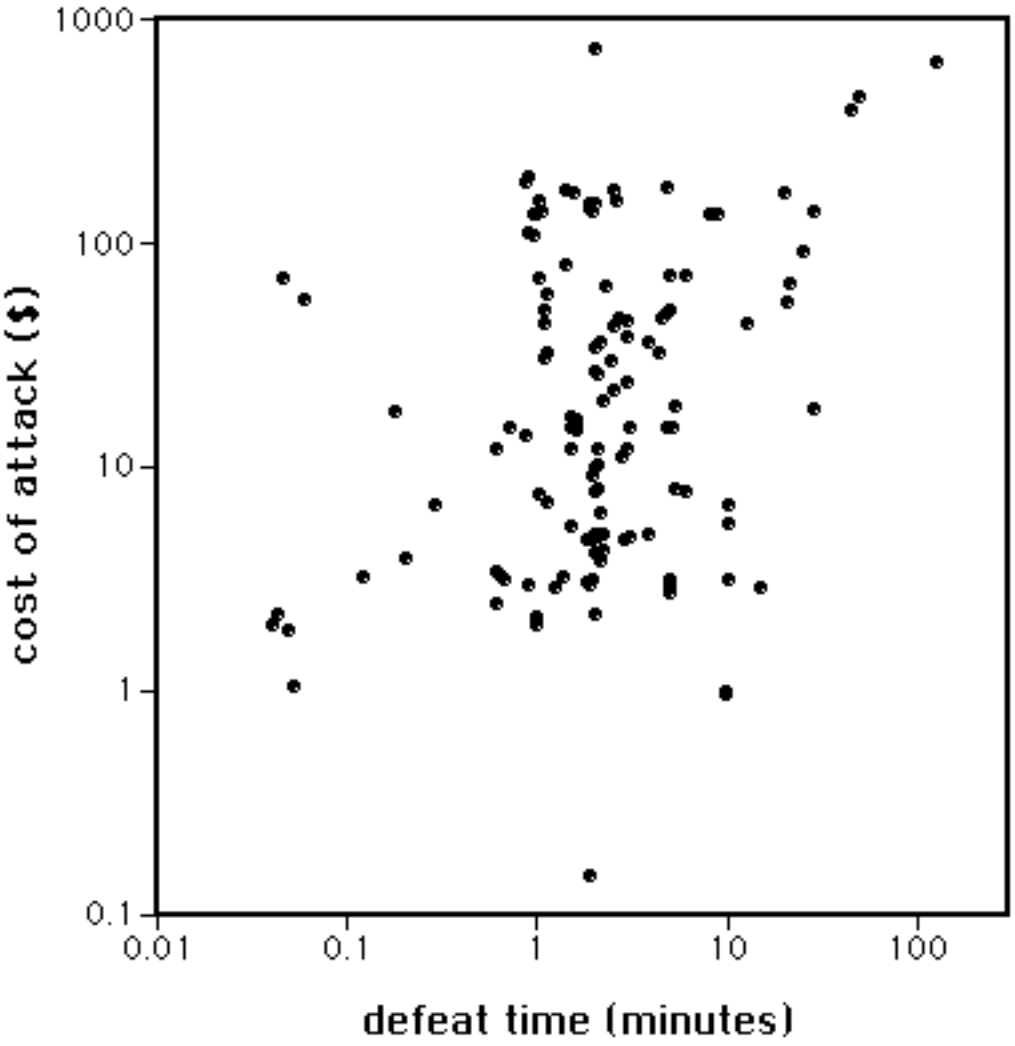

Figure 4 - Estimated Cost of Equipment, Tools, and Supplies for Defeating a Seal as a Function of Defeat Time.

About the Author -- Roger Johnston is a Project and Team Leader in the Chemical Science and Technology Division at Los Alamos National Laboratory, and serves on the Laboratory's Science and Engineering Advisory Council. He received a B.A. from Carleton College in 1977, and M.S. and Ph.D. degrees in experimental physics from the University of Colorado in 1983. Dr. Johnston's technical interests include laser applications, biotechnology, biometrics, and security technology. He holds 3 U.S. patents and is the author of 37 technical papers and 15 invited talks. Dr. Johnston has received two national R&D 100 Awards, a "Best of What's New" Award from Popular Science, a LANL Distinguished Performance Award, and a Los Alamos Excellence in Enterprise Award for technology transfer. He is a member of ASIS.

About the Author -- Anthony R.E. Garcia is a senior mechanical technician in the Chemical Science and Technology Division at Los Alamos National Laboratory. He is the author on 25 technical papers, and has contributed to research and development projects involving national security, superconductivity, thin film physics, and laser applications. His work on vulnerability assessment of tamper-indicating devices led to a 1995 Los Alamos Distinguished Performance Award and a 1996 Achievement Award.