LA-UR-96-3827

Title:

Physical Security and Tamper-Indicating Devices

Author(s):

R.G. JOHNSTON
A.R.E. GARCIA

Submitted to:

http://lib-www.lanl.gov/la-pubs/00418767.pdf

Los Alamos
NATIONAL LABORATORY

Physical Security and Tamper-Indicating Devices

Roger G. Johnston and Anthony R.E. Garcia

Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565
Los Alamos, NM 87545
phone: 505-667-7414
email: roger_johnston@lanl.gov

Abstract

Computer systems, electronic communications, digital data, and computer storage media are often highly vulnerable to physical tampering. Tamper-indicating devices, also called security seals, can be used to detect physical tampering or unauthorized access. 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

Physical security is a crucial component of overall security, privacy, and integrity for computer systems, electronic communications, digital data, and computer storage media. These must ultimately be coupled physically to the external world. The physical coupling can be exploited by an adversary for purposes of tampering.

Physical tampering is often the weak link in overall security for a number of reasons. Physical attacks usually do not require an understanding of the electronics, algorithms, passwords, encryption, or software that may be in use. Physical attacks can frequently be accomplished with surprisingly little sophistication, time, or skill. Developers and users of high-tech systems also may have expertise in electronics and computer security, but limited experience with physical coupling issues and physical security. Then there is also the common problem of over-confidence in high technology that may lead to a failure to seriously consider simple, low-tech vulnerabilities.

Tamper-indicating devices, also called security seals, can have an important role to play in physical security (Staehle, 1992; Rosette, 1992; Horton and Waddoups, 1995; Johnston, Garcia, and Grace, 1995). Seals are intended to leave unambiguous, non-erasable evidence of unauthorized physical entry or tampering. Unlike locks, seals are not meant to prevent physical access, just to record the fact that it has occurred.

The Vulnerability Assessment Team at Los Alamos National Laboratory has undertaken an analysis of 94 different security seals. This study has generated some surprising findings. The purpose of this paper is to share these generic findings, as well as some of our thoughts about physical tamper detection.

Vulnerability Assessment of Seals

Security seals take a variety of different forms (Staehle, 1992; Rosette, 1992; Horton and Waddoups, 1995; Johnston, Garcia, and Grace, 1995; ASTM, 1988). 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.

The 94 tamper-indicating devices that we have analyzed include both commercial and government-developed security seals. Most are in wide-spread use in industry and by the United States Government, including for critical applications.

The work reported here is an extension of the vulnerability assessments of 79 security seals previously reported (Johnston, Garcia, and Grace, 1995; Johnston, 1996).

Table 1 shows the types of seals analyzed in this study. Of the 94 different products studied, 3 were electronic and 91 were passive. A passive seal is one that requires no internal or external electrical power.

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

We devised and demonstrated between 1 and 3 different defeats for each of the 94 seals we analyzed, for a total of 132 defeats. "Defeating" a seal means gaining access to whatever it is protecting without leaving behind evidence of this entry that can be detected by the inspection protocol used for that seal.

All 132 demonstrated defeats were physical and based on low-tech attacks. We define a low-tech attack (Johnston, 1997a and 1997b) 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. Some of the defeats required considerable practice and/or skill with the hands at the level of an average artist or artisan. Many did not.

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.

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.

Table 2 summarizes the defeat times and cost of the 132 demonstrated defeats. The defeat time is the time required 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 perform certain aspects of the defeat in parallel.

Table 2 - Summary of the defeat time and cost for the 132 demonstrated defeats.

	mean	minimum	maximum
defeat time	4.3 mins	3 secs	125 mins
cost of defeat	$56	$0.15	$750

The low-tech nature of the attacks is emphasized by the modest cost figures shown in Table 2. The cost for each defeat was an estimate for all the equipment, tools, supplies, and services (e.g., machining in a commercial machine shop) needed to implement the attack once. The marginal cost for each defeat--that is, the cost to defeat a second seal using the same attack scenario--is substantially less. This is because many of the equipment, tools, and supplies involved in an attack can be reused for another attack on the same type of seal.

Table 3 shows the correlation for each of the 132 demonstrated defeats between the unit cost of the seal (in quantities of 1000), the time to complete the defeat, and the cost of a single defeat.

Table 3 - Correlation between various defeat parameters. The value r is the Pearson linear correlation coefficient.

parameter y vs. x	r	mean dy/dx
defeat time vs. unit cost	0.08	1 sec/dollar
defeat cost vs. unit cost	0.31	50 cents/dollar
defeat cost vs. defeat time	0.60	$5/minute

The correlation between the defeat time and the cost of the seal is so weak (r=0.08) 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.

The third column (dy/dx) in Table 3 also shows that more expensive seals do not require significantly more expensive attacks and that, on average, each extra minute required to complete a defeat is accompanied by only a $5 increase in the cost of the tools, materials, and supplies needed for the attack.

Discussion

There are some serious limitations and problems associated with any kind of vulnerability assessment of security devices, including this work. These are discussed in some detail by Johnston (1996, 1997a, and 1997b), Johnston, Garcia, and Grace (1995), and ASTM (1988).

Despite these problems and limitations, this work raises some interesting issues. We found that all 94 seals we studied can be defeated quickly and inexpensively using low tech methods and highly portable (usually concealable) tools and supplies. It is also surprising that there appears to be little correlation between defeat time and the cost of a seal, or between the cost of an attack and the cost of a seal. One might intuitively expect that more expensive seals would be better able to withstand attack. Apparently this is not generally the case.

For most of the seals, we believe that minor, low-cost modifications to the seal would substantially increase the difficulty of attacks. Most seals would also benefit significantly from changes in the manufacturer’s or user's protocol for procurement, storage, installation, inspection, removal, disposal, and training. Most of the changes we would suggest are relatively minor. Some are highly application-dependent. For many of the seals, we believe that having security personnel aware of the most likely attack scenarios, and watching for them, would dramatically improve tamper detection.

Persons with a legitimate interest in physical security are welcome to contact us to discuss vulnerability issues in more detail.

Acknowledgements

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

References

Horton, P.V. and Waddoups, I.G. (1995). Tamper-indicating devices and safeguards seals evaluation test report SAND93-1726/2. Albuquerque, NM: Sandia National Laboratories.

Johnston, R.G., Garcia, A.R.E., and Grace, W.K. (1995). Vulnerability assessment of passive tamper-indicating seals. Journal of Nuclear Materials Management, 2,224.

Johnston, R.G. (1996). Vulnerability assessment of commercial and government tags and seals. In M. Farrar (Ed.), Proceedings of the ASIS/DoD security seals and tamper-indicating device symposium (pp. 25-36 and 55-71). Port Hueneme, CA: Naval Facilities Engineering Service Center.

Johnston, R.G. and Garcia, A.R.E. (1997a). Vulnerability assessment of security seals. Journal of Security Administration (in press).

Johnston, R.G. (1997b). Effective vulnerability assessment of tamper-indicating seals. Journal of Testing and Evaluation (in press).

Rosette, J.L. (1992). Improving tamper-evident packaging. Lancaster, PA: Technomic Publishing.

Staehle, G. (1992). DOE's Tags and Seals Program, In G. Staehle (Ed.), Verification technologies: Report DOE/DP/OAC/VT-94B (pp. 1-41). Washington, DC: United States Department of Energy.

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