Edith Cowan University
Research Online

Australian Security and Intelligence Conference | Security Research Institute Conferences

2010

A Comparison of Laboratory and Vulnerability Evaluation Methods for the Testing Security Equipment

Benjamin Beard
Edith Cowan University

David J. Brooks
Edith Cowan University

Originally published in the Proceedings of the 3rd Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 30th November 2010
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/asi/1

A Comparison of Laboratory and Vulnerability Evaluation Methods for the Testing Security Equipment

Benjamin Beard[2] and David J. Brooks[1,2]
[1] secau – Security Research Centre
[2] School of Computer and Security Science
Edith Cowan University
Perth, Australia
bjbeard@student.ecu.edu.au, d.brooks@ecu.edu.au

Abstract

A facility wide security system cannot be tested without causing disruption or creating vulnerabilities within the system. To overcome this issue, individual components or equipment may be evaluated to a priori performance standard. The two common approaches to security equipment evaluations are vulnerability attacks and laboratory testing. Laboratory testing of security equipment can reduce the costs and time associated with evaluations, as well as limiting the subjectivity of the tests. Vulnerability attacks will produce more realistic evaluation results of the whole security system; nevertheless, the data obtained is dependent on the physical attributes and skill of the attackers.

This study ascertained what methodology, namely laboratory testing or vulnerability testing, was the most effective. To achieve this, both testing methodologies were applied to security padlocks with expert validation. The study confirmed that if security equipment has been laboratory tested to a designed priori performance level, the degree of security vulnerability can be effectively identified. As the security padlocks demonstrated, the high level achieved in the laboratory tests correlated with a high delay factor in vulnerability testing. Such an approach to security equipment testing resulted in a reliable and valid quantitative data set that could be applied at a later stage to other similar equipment. Nevertheless, it is suggested that when considering a facility wide security system, some degree of both laboratory and vulnerability testing has to be applied as they are complimentary.

Keywords

Laboratory, evaluation, testing, equipment, vulnerability, methodology

INTRODUCTION

The development of novel security measures is a well-documented field; however, research often overlooks the deployment of such security measures. The effectiveness of a security measure in meeting its objectives should be understood and documented in order for protective security measures to be better designed, applied and managed. Security equipment evaluations are carried out on a variety of technologies, using many different methodologies. Government departments, commercial organisations and academic institutions all conduct security equipment evaluations to varying degrees and using a variety of methods.

Two of the most common security evaluation methodologies are *laboratory testing* and *vulnerability testing*. Laboratory testing or *simulated methods* can reduce the impact of financial costs and time constraints associated with security equipment evaluations. Vulnerability testing or *adversary attacks* will produce more realistic evaluation results, but the data obtained is dependent on the physical attributes and skills of the attackers. Each method of evaluation has many advantages and disadvantages, and this study seeks to explore the relationships between each method.

BACKGROUND OF THE STUDY

Security equipment testing and evaluation have been an important element for the treatment of security risks (Jones & Smith, 2005, p. 20). A risk management plan is disadvantaged if the effectiveness of the risk mitigating measures are unknown. Security assessment theories—such as critical path analysis—require quantitative data from evaluation results, which leads to a more effective security system.

In general, the level of evaluation applied to security equipment focuses on electronic or detection devices. Such an approach are attributed to a number of factors, including the on-going development of the base technology, the repeatability of tests and the relative safety of the evaluations; however, the evaluation of physical security equipment is a less documented field. The tools and skills required for evaluations of physical security

equipment makes them restrictive to undertake. Issues of cost and safety also limit the application of such evaluations. The destructive testing of physical security equipment is under-reported, perhaps in part due to the large outlays required to achieve scientific and statistical accuracy. In addition, evaluation groups who conduct physical security tests rarely publish results in the open source domain, as clients may require a level of confidentiality with the test results or equipment vulnerabilities.

PURPOSE OF THE STUDY

The purpose of this study was to:

- Conduct applied laboratory testing of security equipment
- Conduct applied vulnerability testing of security equipment
- Compare and contrast testing methods and results
- Define what testing methodology achieves the most effective security evaluation result

There are numerous advantages of using a security equipment testing and evaluation framework, with a methodical and analytical process (Jones & Smith, 2005). Nevertheless, published scientific results that validate the proposed approach should support testing models. In addition, evaluations should be valid and reliable in evaluating the effectiveness of security equipment (Wassell, 1999, p. 90).

REVIEW OF LITERATURE

Academic studies often overlook applied security measures, whilst focusing on developing security technologies. The effectiveness of a security measures in meeting its objectives needs to be understood and documented in order to efficiently design and manage protective security measures. Approaches to assess the effectiveness of security controls may include:

- Estimating the efficiency and weaknesses of the security system against the threats
- A *Red team* style of mock attack exercises against generic threat types
- Simulated target analysis against specific threat methods
- A US military CARVER method (Standards Australia, 2006, p. 65)

In general, security equipment evaluations are conducted infrequently, with minimal consideration of validity and reliability. The relative immaturity of the supporting science means that most evaluations are only conducted by government authorities that have the appropriate funding; however, there are some additional commercial and academic institutes completing security equipment evaluations. In addition, almost all of these conducted evaluations centre on a defined standard or criterion.

Government evaluation

Many government bodies conduct evaluations on security equipment. A variety of methodologies, criteria and theories are used. In Australia, the Security Construction and Equipment Committee (SCEC) is an interdepartmental committee of government that oversees the evaluation and approval of security equipment across whole-of-government (ASIO, 2006, p. 1). ASIO T4 Protective Security tests protective security products to determine their suitability for use in Australian government facilities on behalf of SCEC. Such testing involves validating claims made by the manufacturers, assessing suitability for specific applications and identifying any limitations or vulnerabilities (ASIO, 2009, p. 1).

The United Kingdom's Home Office Scientific Development Branch (HOSDB) evaluates many types of security equipment to ensure that they are suitable for use by the UK government and critical infrastructure (Armstrong, 2005, p. 1). HOSDB conducts both scientific and attack tests, and significant work has been undertaken in the field of perimeter intrusion detection (PIDS) systems (Tarr, Leach, & Branch, 1998, p. 196). The UK Centre for the Protection of National Infrastructure (CPNI) also manages a research and evaluation program into science and technologies aimed at improving the security of national infrastructure, including physical, personnel and electronic security (CPNI, 2009, p. 1).

In the United States, Sandia National Laboratories has been conducting research and security evaluations for over 30 years on behalf of the US Government's Department of Energy (Garcia, 2001, p. 1). Evaluations of protective security systems are undertaken to ensure the integrity of US nuclear assets and research is conducted to support many aspects of the US administration (Sandia Corporation, 2009, p. 1). For non-government

organisations, there is often minimal guidance on the application of protective security measures. In addition, there is also reliance placed on manufacturers' claims, third-party security consultants and other forms of empirical evidence. Nevertheless, as government guidance is developed and disseminated, such knowledge will define what measures are practicable and effective (Claber, 1998b, p. 73).

Commercial and academic evaluation

Governments may lead the way with security equipment evaluations; nevertheless, some commercial and academic entities have realised gains through evaluating security products within their own facilities or in partnership with government institutions. Senstar Stellar, a manufacturer of security equipment, operates the Sensor Integrated Test Environment in Ottowa, Canada. Their facility is used for the evaluation and development of Senstar Stellar's own products (Jones & Smith, 2005, p. 30; Maki, Hill, & Malone, 1999, p. 113). South West Microwave have also conducted security equipment evaluations, in conjunction with the US Corrective Services (Harman, 1998, p. 150). The Gryffin TALOS taut wire PIDS was evaluated by the manufacturer in a laboratory style environment using computer simulations, interfaced directly to the sensor device (Hellard, 1998, p. 209).

Security equipment evaluations are undertaken by some academic institutions. As with commercial evaluations, these activities are often completed in conjunction with government or private enterprise. The Security Systems Research and Testing Laboratory (SSRTL) at Edith Cowan University, Western Australia, commenced evaluations in 2004 and has since completed work with intelligent CCTV systems, biometric devices (Brooks, 2009), development of testing procedures, and integrated evaluation and risk analysis models (Smith, 2005, p. 4). One such model is the Jones and Smith Model of Security Equipment Testing and Evaluation, which combines risk management principles with scientific evaluations for security equipment (Jones & Smith, 2005, p. 32). Another approach from the same laboratory is the defeat evaluation methodology used to evaluate an "insider" vulnerability with biometric access systems (Brooks, 2009). The Southwest Surety Institute is a partnership between Sandia National Laboratories and several universities in the United States. Evaluations conducted by this group include assessment of protective security systems, PIDS, computer modelling of equipment performance and blast mitigation measures (Garcia, 1998, p. 232).

Recently, a new form of vulnerability testing has emerged via the internet community. For example, the Locksport community exploits many locking devices with their results disseminated through such mediums as *YouTube* and conferences, such as DEFCON in the USA (shadowswan, 2006).

Standards

Standards currently used in the evaluation of physical security equipment include locking devices, barriers, building elements, security containers, glazing and ballistic resistant elements. Standards may be considered "published documents setting out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform" (Standards Australia, n.d., p. 2). Such an approach ensures that a common *language* is achieved within industry, driven by the more progressive parts of industry, legislation and community expectations.

One such organisation that develops and propagates security standards is *Standards Australia*. Standards Australia is Australia's peak standards organisation, although they are a public company limited by guarantee. The organisation is charged by the Australian Commonwealth Government to provide general oversight and governance of Australian Standards (Standards Australia, n.d.). Their four key areas of focus include national and international coordination, accreditation of other organisations to produce standards, development and update of standards, and design assessment (Standards Australia, 2009).

Standards used for security equipment evaluation can include both the method of testing and/or the classification of products based upon the test results (Claber, 1998a, p. 70). Some standards for physical security equipment include, but are not limited to:

- Australian Standard AS4145-2002 Locksets
- Loss Prevention Council LPS1175
- Sold Secure SS 304
- Home Office Scientific Development Branch (HOSDB) Physical Barrier Attack Standard

THEORY SUPPORTING THE STUDY

A facility wide security system cannot be exhaustively analysed without causing widespread disruption or creating vulnerabilities during testing. For this reason, the evaluation of individual components to a performance standard is necessary. If a security system is found to be ineffective through evaluations of its individual components, then vulnerabilities within the system may be identified (Garcia, 2001, pp. 5-6). However, security equipment evaluations can be a costly and time-consuming process. Therefore, it is important that evaluation data can be transferred and compared between different categories of security equipment (Armstrong & Peile, 2005, p. 1). To achieve this outcome, rigorous quantitative evaluations are required for security systems that protect assets with a significant national or community consequence (Garcia, 2001, p. 241). In addition, on-going evaluation of security equipment by independent sources will overcome industry issues of poor quality purchases and installations (Paget, 1998, p. 201).

Computer simulations of real life sequences to some types of security equipment, most notably detection devices, can be applied. Although these methods will quicken research and development opportunities, they are not a true substitute to vulnerability tests in real life situations (Hellard, 1998, p. 209). Evaluations and standards should be based upon the principles of impartiality, objectivity, reproducibility (precision when the evaluation is reproduced by other parties), reliability, validity and accuracy (Armstrong & Peile, 2005, p. 1). Nevertheless, threat sources are flexible and frequently alter attack methods due to installation of security measures (Claber, 1998b, p. 73). For this reason, evaluations should also be extended to the human element of a protective security system, such as the efficacy of x-ray screening operators at an airport or the speed of an on-site response force to an alarm activation (Klock, 2005, p. 1).

APPROACHES TO EQUIPMENT EVALUATION

It is important that evaluation and standards for security equipment is specific enough to cover possible variables of the technology, achieved through a number of evaluation methodologies (Armstrong & Peile, 2005, p. 2). The performance of element's in a protective security system, whether fulfilling deterrence, detection, delay or response functions cannot be truly verified without a one hundred percent end-to-end test. If such an approach is taken, entropic decay has already been introduced into the security system (Coole & Brooks, 2009). Nevertheless, end-to-end evaluation when installing and operating a protective security system is not considered because of financial and time constraints (Brown, 1998, p. 225).

In-field testing

There are four different types of *in-field* testing, namely pre-delivery testing, contractors field-testing, performance verification testing and endurance testing. Pre-delivery testing describes evaluation of a protective security system element that is conducted prior to its installation, usually undertaken by the equipment manufacturer. Such testing can verify the performance of individual components of the equipment, as well as overall effectiveness. Contractors field testing is most often conducted by the manufacturer or retailer of the product, with a series of tests to verify performance requirements once site installed (Brown, 1998, p. 227).

Performance verification testing—similar to the vulnerability testing undertaken in this study—should completely evaluate all components of the security equipment to their limits. A thorough on-site evaluation of the equipment by the owner will confirm that contractual obligations have been met by the installer, as well contribution to vulnerability and security risk assessments (Brown, 1998, p. 228). If simulated due to constraints, vulnerability testing should replicate real world conditions as closely as possible (Jones & Smith, 2005, p. 24).

Endurance testing relates closely with the outcomes of performance verification testing. Although this type of testing is most applicable to electronic detection devices in a protective security system, it can also evaluate some types of equipment that provides physical delay. Longitudinal analysis of false acceptance rate (FAR) for a detection system, or cyclic testing, would be examples of endurance testing (Brown, 1998, p. 228). Not all aspects of on-site testing are applicable to the complete protective security system. To test many physical elements against expected attacks would be impractical in both time and cost; however, some assurance of equipment performance against real life attacks will always be required (Brown, 1998, p. 229).

Jones and Smith Model

The Jones and Smith Model of Security Equipment Testing and Evaluation, intrinsically links the security risk management process with that of equipment evaluation. Following the *threat* assessment and risk identification stages of security risk management, requirements for the performance of security equipment should be drafted by the risk owner (Standards Australia, 2006, p. 70). Such an approach proceeds two levels of security equipment evaluation, with level 1 testing within a controlled laboratory environment. Level 2 is a simulated vulnerability testing that should replicate real-world conditions as closely as possible (Jones & Smith, 2005, p. 24). The information from both stages of testing feeds back into the risk process, with consideration of expected threats.

Vulnerability and laboratory testing

It can be seen that two common approaches to security equipment evaluations are laboratory testing and vulnerability attacks. Laboratory testing or 'simulated methods' can reduce the impact of financial costs and time constraints associated with security equipment evaluations. This form of evaluation also limits the subjectivity of the tests (Armstrong & Peile, 2005, p. 3). Vulnerability attacks will produce more realistic evaluation results, nevertheless, the data obtained is dependent on the physical attributes and skills of the attackers (Armstrong & Peile, 2005, p. 3). One example of simulated real-life conditions is the use of an on-site test to evaluate PIDS performance. By using a calibrated impact device at pre-determined points on a fence, scientific and repeatable results can be obtained from equipment installed in a protective security system (Leach & Horner, 1997, p. 25).

The effectiveness of security equipment in specific applications cannot be determined by manufacturer sourced information alone. The equipment must be evaluated by unbiased groups to obtain accurate evaluation data (Paget, 1998, p. 204). The lack of a scientific approach to evaluate security equipment will only provide crude results and the ability to make approximate decisions (Williams, Berentsen, & Rexfort, 1999, p. 95).

THE STUDY

The study attempted to ascertain what methodology, namely *laboratory testing* or *vulnerability testing*, was the most effective within the context of this study. To achieve this, both methods were applied to a number of *security padlocks* and measures taken. The study applied a staged process, where pre and post expert interviews were carried out following or proceeding physical laboratory and vulnerability testing (Figure 1).

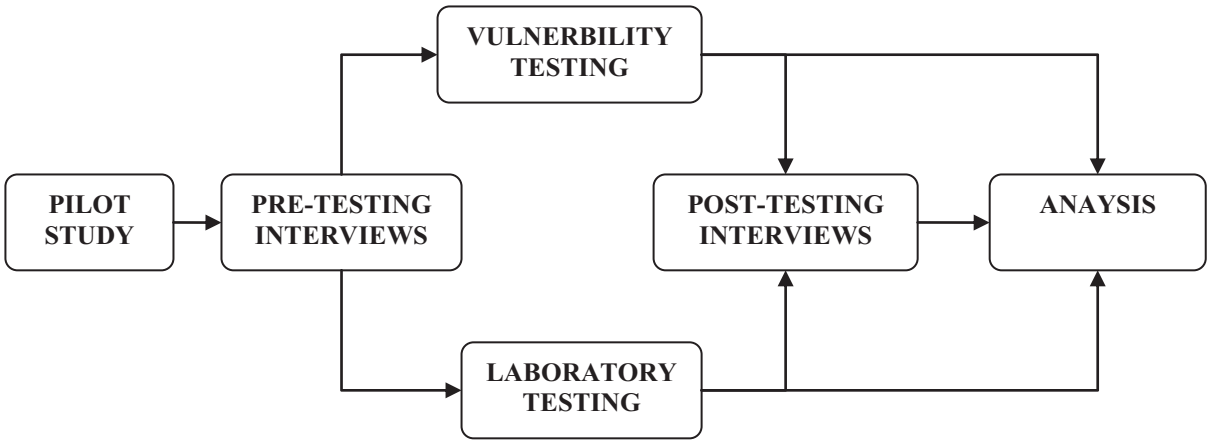


Figure 1: Study design

The structured interviews were conducted with security equipment evaluation experts to ascertain the most efficient and safest way of conducting the vulnerability and laboratory testing. Then, in accordance with the Australian Standard, laboratory testing of the padlock shackles demonstrated the resistance of the shackles to a bolt-cutter style attack. These results were compared and contrasted with those of the vulnerability testing, where the shackles were tested in as close to real life condition as possible. Repetition of both laboratory testing and vulnerability attacks offered a much more accurate and valid set of results obtained (Armstrong, 2005, p. 3). Such an approach allowed data collection in a reliable and valid manner, and then be compared to an established Australian Standards AS4145.4:2002. Finally, the results of both data sets were subjected to expert opinion

through structured interviews. These interviews assessed validity, reliability and the perceived relationship between laboratory and vulnerability testing. To ensure that no commercial impact resulted from publication of the performance data, the padlocks used for this study were referred to as Padlock A and B.

Evaluation of a security padlocks

A performance measure for any delaying security control is the time needed to defeat the measure (Garcia, 2001). The measure of delay effectiveness is the time that an attacker requires to bypass each element of delay. However, any delay provided by security controls prior to detection is of minimal benefit as it does not assist the response force in interdicting the intruder (Garcia, 2001, p. 7). Therefore, the evaluation of physical barriers are required to determine the overall effectiveness of a protective security system.

Padlocks and chains are inherently susceptible to physical attack. If possible, padlocks and chains should be avoided as a means of securing assets; however, there are some products that will provide larger delay against manipulation and physical attack (ASIO, 2006, p. 15). A common attack method against padlocks and chains is the use of bolt cutters or croppers, with the resistance of padlock shackles to this attack may be evaluated in AS4145.4. This Australian Standard may be applied in measuring security padlocks effectiveness, as it stipulates that when testing the resistance of the padlock shackle to cutting attacks, a force meter should be used in conjunction with specially designed test jaws. The jaws should be made from general tool steel with a hardness of 60-62 Rockwell Steel Hardness (HRC). The dimensions of the jaws should form a 1.5mm flat point, then taper away at 60° to a width of 14mm (Standards Australia, 2002, p. 22).

In AS4145.4 ten physical security grades (SP) are employed for padlocks, ranging from the lowest SP1 resistance to attack to the greatest SP10. These grades are defined, in part, by 14 categories such as minimum number of effective key differs, minimum number of effective combinations, resistance to force on cylinder plug or locking mechanism, resistance to pulling, resistance to cutting of shackle, resistance to drilling of padlock body, shackle and staple, etc., (Standards Australia, 2002).

Laboratory testing

The methodology for the laboratory testing was developed through Australian Standard AS4145.4 and discussions with security equipment evaluation experts. The padlocks were evaluated using a cutting jig (Figure 2). A compressive extension test applied pressure to the cutting jaws and onto the padlock, until one of the end of test parameters occurred. These parameters were a 30% change in the applied force or a preset extension that stopped the jaws from damaging themselves after crushing through the padlock shackle. To minimise costs associated with the testing, only one padlock was sourced for each sample set. After each conducted test, the shackle was removed and catalogued, and a new shackle installed into the padlock and repeated 30 times for each sample set.

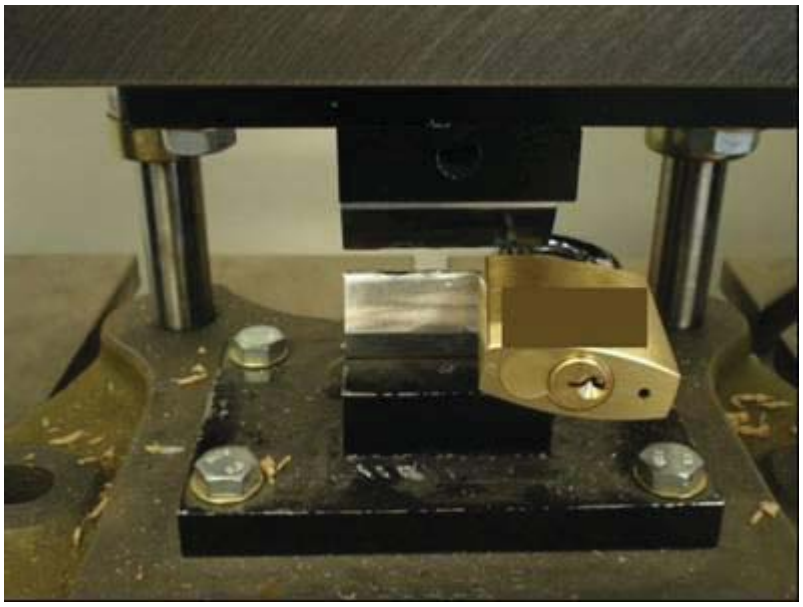
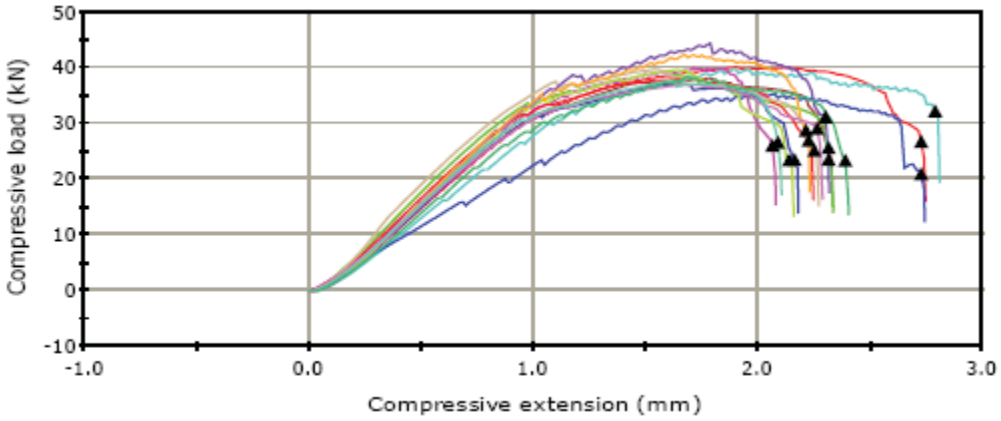


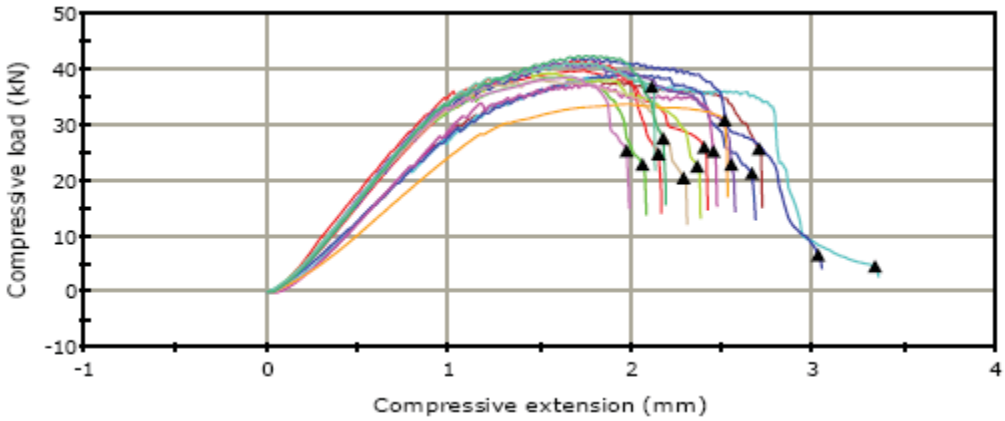
Figure 2: Padlock shackle testing jig with padlock shackle

Padlock A

The laboratory testing for Padlock A resulted in a mean value of 39.13kN (SD 2.17kN) obtained from thirty repetitions (Graphs 1 and 2). This measure was equivalent to physical security grade SP7 in the Australian Standard AS4145.4:2002 (Standards Australia, 2002, p. 20).



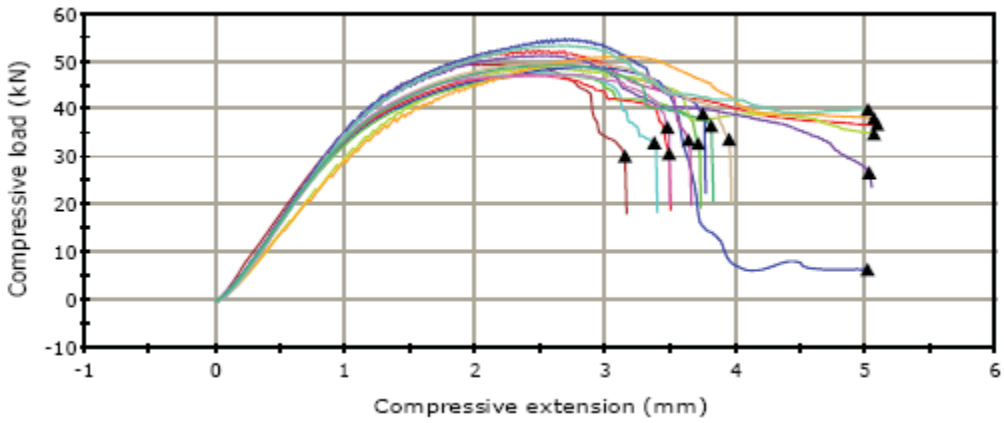
Graph 1: Padlock A, repletion tests 1 to15



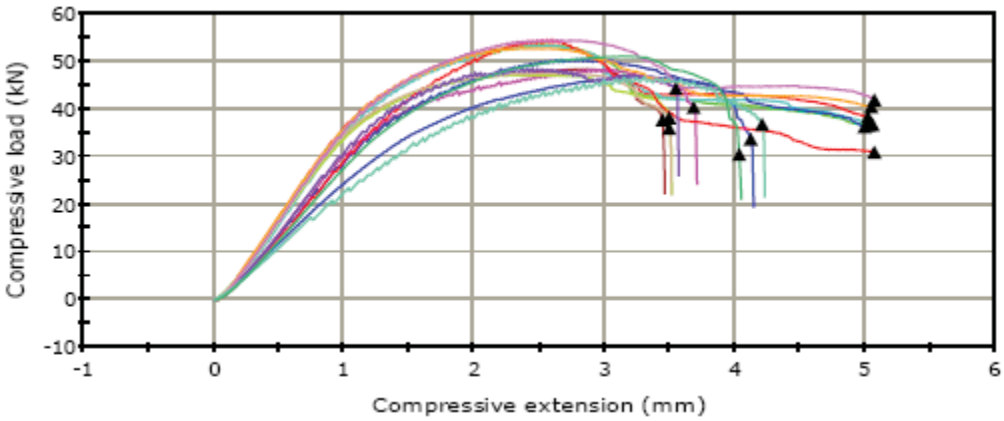
Graph 2: Padlock A, repletion tests 16 to 30

Padlock B

The laboratory testing for Padlock B resulted in a mean value of 50.03kN (SD 2.62kN) obtained from thirty repetitions (Graphs 3 and 4). This measure was equivalent to SP8 in the Australian Standard AS4145.4:2002 (Standards Australia, 2002, p. 20).



Graph 3: Padlock B, repletion tests 1 to 15



Graph 4: Padlock B, repletion tests 16 to 30

Vulnerability testing

The vulnerability tests obtained quantitative data on the resistance of the padlock shackle to bolt cutter attacks. The padlock shackles were subjected to bolt cutter attacks in simulated real life conditions. The defeat times achieved in the vulnerability attacks may have been dependent upon the strength and skills of the attacker (Armstrong, 2005, p. 4). For this reason, there was a session for attackers to familiarise themselves with the tools and attempt a few practise attacks. This vulnerability stage of testing used a bench mounted vice and 750mm bolt cutters (Figure 3).

Figure 3. Vulnerability testing toolset, with 750mm bolt cutters on right.

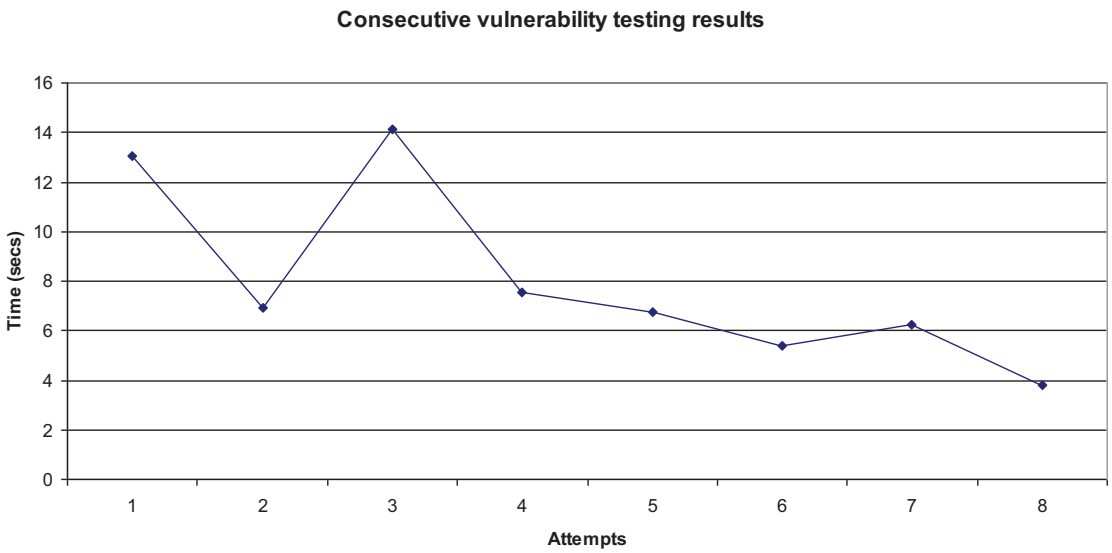
The padlocks were attached to a chain and the chain was placed into the bench mounted vice (Figure 4). Each attempt at a cutting attack was made with the 750mm bolt cutters, with results observed, timed and recorded.

Figure 4: Padlock shackle vulnerability test setup

For vulnerability testing, one sample from each set was tested alternatively. Padlock A resulted in a mean value of 5.91sec (SD 1.66sec) obtained from four repetitions. The testing for Padlock B resulted in a mean value of 10.03sec (SD 4.13sec) obtained from four repetitions. Whilst attempting the fifth Padlock B repetition (the ninth total repetition) the bolt cutters sustained damage that stopped further testing.

As more attacks were undertaken, the attackers' technique and speed improved for both sets of padlock shackles (Graphs 5 and 6). If further testing were possible, it is foreseeable that this improvement would continue to some degree. Comments from participants in both sets of interviews listed fatigue as a variable in the vulnerability testing.

Graph 5: Vulnerability testing results (Sample sets)



Graph 6: Vulnerability testing results (combined results of both padlocks)

Expert interviews on testing

The expert opinions had a tendency to focus on the difficulties and variables experienced with security equipment evaluations. These difficulties were demonstrated through the literature on the subject and the data obtained. Garcia stated that a facility wide security system cannot be exhaustively analysed without causing widespread disruption or creating vulnerabilities during testing (2001, p. 5). If a security system is found to be ineffective through evaluations of its individual components, then vulnerabilities within the system can be identified (Garcia, 2001, p. 6). The restrictive time and costs associated with some security equipment evaluations are documented in the literature (Armstrong & Peile, 2005). The laboratory and vulnerability testing mirrored these themes, as it was difficult to conduct highly accurate or destructive testing on the padlocks if they were in use within a security system. The damage caused to the bolt cutters during the vulnerability testing in the both the pilot and primary studies caused the testing to be halted, as replacement of the tools would make the study expensive. In addition, the financial costs to obtain the padlocks and shackles were significant for a study of this size and evaluation of more expensive security equipment could put studies one out of reach for most institutions.

The analysis of the post testing interview responses demonstrated that 80 percent of the participants thought that combining the two testing methods for each evaluation and developing a comprehensive evaluation model could, and should, be done. This view was reflected by the relationship between the testing results. The laboratory testing results indicated that Padlock B was stronger than Padlock A and the experts interviewed also recognised the significance of that relationship, especially when it was reflected in the vulnerability testing results. Those results indicated that Padlock B provided more delay against the bolt cutter attacks. Therefore, the relationships between expert opinion and the testing results support the amalgamation of both methods of testing for security equipment evaluations.

The similarity between both the pilot and primary study results indicated that the methods used were reliable. The laboratory testing results demonstrated comparatively low standard deviations over the whole testing series. The vulnerability testing for both studies had a failure of the bolt cutters, indicating a trend in the overuse of the equipment.

RECOMMENDATIONS

The data and analysis from this study can be used to make several recommendations for security equipment evaluations. The relationships between vulnerability testing and laboratory testing are complimentary, rather than predictive, meaning that where applicable evaluations should incorporate both types of testing. Such a model would use laboratory testing to ascertain if the equipment meets an industry or standards benchmark. Vulnerability testing can then explore and identify any other weaknesses in the equipment. Such an approach

could ensure that evaluated equipment is statistically reliable, environmentally fit-for-purpose and mitigates against expected threats.

The study confirmed that the level of security vulnerability was affected if equipment has been evaluated. The Padlock A demonstrated properties equivalent to AS4145.4-2002 physical security grade SP8 and Padlock B grade SP7. The higher grade achieved by Padlock A in the laboratory tests correlated with a higher delay factor in vulnerability testing. Many standards that deal with security equipment focus solely on laboratory testing, as it is easier to conduct and provides quantitative results. However, the introduction of vulnerability testing to many of these standards could improve the resistance of security equipment to evolving and original attack methods.

As the study has demonstrated with the sample padlocks, laboratory evaluation allowed isolated tests of system components, in a time and cost efficiency manner. Such testing resulted in a reliable and valid quantitative data set that could be applied to other similar product. Whereas vulnerability testing allowed the many individual components to be tested as a holistic system, directed by the attackers capabilities. By combining the two evaluation methods in a formal methodology, more robust security systems that are relevant to the assessed threats may be designed, applied and managed. Such an approach was supported by Jones and Smith in their *two level* security equipment evaluation model that applied a controlled laboratory environment and a simulated vulnerability test (2005, p. 24).

Finally, such testing provides a scientific approach to security evaluation, where reliability and validity are considered and applied. As Armstrong suggests, repetition of both laboratory testing and vulnerability attacks will offer a much more accurate and valid set of obtained results (2005, p. 3). Such an approach allows the design and application of security systems, with a known and measurable weakness of each single component leading to an understanding of the whole system. A systems approach allows a quantitative measure of system performance to be defined, where continuous measures can be applied and monitoring reduces entropic security decay (Coole & Brooks, 2009).

CONCLUSION

This article has presented a study that attempted to define what approach may be the most effective when evaluating either a facility wide security system or security components, devices or elements. Such evaluations should result in a reduction in system vulnerabilities, gained by better understanding and application of equipment into a system. The study considered two evaluation methods, namely *laboratory testing* and *vulnerability testing*, applied to security padlocks. Evaluation tests provided data that were used to establish the relationships between laboratory and vulnerability testing in security equipment evaluations. Although analysis of comparative effectiveness is to some degree a subjective process, such comparison can provide useful interpretation.

The comparative results between the laboratory and vulnerability tests demonstrated a strong correlation between high levels of resistance to laboratory testing and subsequent reduced equipment vulnerability. The vulnerability attacks were effectively defeated, due to the strength of the security padlocks. Such results indicated that the design of security equipment to a priori laboratory testing standard would reduce vulnerability levels, provide quantitative data for other similar security equipment and both methodologies of testing are complementary. In addition, such evaluation allows more effectively designed and applied facility wide security systems.

REFERENCES

Armstrong, D. (2005). A Model for the Evaluation of Barriers and Containers and Their Resistance to Physical Attack. Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on, 1-4.

Armstrong, D., & Peile, C. (2005). Perimeter Intruder Detection Systems Performance Standard. Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on, 1-4.

ASIO. (2006). SEC 2006 Security Equipment Catalogue. Canberra: Commonwealth of Australia.

ASIO. (2009). Protective security and T4 Retrieved 05/06/09, from http://www.asio.gov.au/Work/content/ProtectiveSecurity.aspx

Brooks, D. J. (2009). Defeating biometric fingerprint systems: An applied testing methodology. Paper presented at the Proceedings of the 2nd Australian Security and Intelligence Conference, Perth.

Brown, J. A. (1998). Don't forget to test![electronic security systems]. Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, 225-229.

Claber, K. J. (1998a). Designing Window Glazing for Explosive Loading. Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, 65-72.

Claber, K. J. (1998b). The Development of Standards for Explosion Protection. Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, 73-78.

Coole, M., & Brooks, D. J. (2009). Security Decay: An entropic approach to definition and understanding. Paper presented at the Proceedings of the 2nd Australian Security and Intelligence Conference, Perth.

CPNI. (2009). Research Retrieved 06/06/09, from http://www.cpni.gov.uk/research.aspx

Garcia, M. L. (1998). Development of security engineering curricula at US universities. Carnahan conference on security technology, Alexandria, VA (United States), 12 Oct 1998.

Garcia, M. L. (2001). The Design and Evaluation of Physical Protection Systems. Boston: Butterworth-Heinemann.

Harman, R. K. (1998). Intrepid update 1998. Security Technology, 1998. Proceedings., 32nd Annual 1998 International
Carnahan Conference on, 147-153.

Hellard, G. (1998). GRYFFIN TALOS taut wire perimeter detection system. Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, 206-209.

Jones, D. E. L., & Smith, C. L. (2005). The development of a model for testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS 4360:2004 - Risk Management. Paper presented at the Recent advances in counter-terrorism technology and infrastructure protection, Proceedings of the 2005 Science, Engineering and Technology Summit 2005 Canberra, Australia.

Klock, B. A. (2005). Test and Evaluation Report for X-ray Detection of Threats Using Different X-ray Functions. Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on, 1-3.

Leach, G., & Horner, M. (1997). Sensitivity variations in linear microphonic cables. Paper presented at the Security Technology, 1997. Proceedings., 31st Annual 1997 International Carnahan Conference on.

Maki, M., Hill, C., & Malone, C. R. (1999). User performance testing of the Perimitrax buried cable sensor. Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on, 112-119.

Paget, M. D. G. (1998). The evaluation procedure for the testing of intruder detection equipment. Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on, 201-205.

Sandia Corporation. (2009). Homeland security and defense Retrieved June 19, 2009, from http://www.sandia.gov/mission/homeland/index.html

Smith, C. L. (2005). The Security Systems Research and Testing Laboratory at Edith Cowan University. Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on, 4-7.

Standards Australia. (2002). AS4145.4-2002 Locksets Part 4: Padlocks Sydney: Standards Australia International Ltd.

Standards Australia. (2006). HB167:2006 Security Risk Management. Sydney: Standards Australia.

Standards Australia. (2009). About us Retrieved July 13, 2009, from http://www.stanrdas.org.au/cat.asp?catid=21

Standards Australia. (n.d.). Image a world without standards. [Brochure]. Sydney: Author.

Tarr, S., Leach, G., & Branch, P. S. D. (1998). The dependence of detection system performance on fence construction and detector location. Proceedings., 32nd Annual 1998 International Carnahan Conference on Security Technology, 1998., 196-200.

Wassell. (1999). Non destructive testing of fence mounted PIDS. Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on, 90-94.

Williams, I., Berentsen, M., & Rexfort, C. (1999). Solid state simulation of movements for the test of volumetric intrusion detectors. Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on, 95-100.