Defensibility and Risk Management

www.hsaj.org/articles/14130

October 2017

Vicki Bier, Alexander Gutfraind, and Ziyang Lu

A common problem in risk management is to characterize the overall security of a system of valuable assets (e.g., government buildings or communication hubs), and to suggest measures to mitigate any security threats. Currently, analysts rely on a combination of security indices, such as resilience (the ability of a system to return to normal rapidly); robustness (the ability to function despite damage); redundancy (spare capacity); security (barriers to limit access); and vulnerability (susceptibility to hazards and/or intentional threats). However, these indices are not always actionable; i.e., they are not themselves sufficient to indicate whether policy makers should invest in improving a given system. Indeed, it has been observed that some vulnerable systems cannot be improved cost-effectively [1].

Motivated by this gap, we recently proposed an index, defensibility [2], which characterizes how easily the damage to a system can be reduced. A system is highly defensible if a modest investment of resources can significantly reduce the damage from an attack or disruption (Fig. 1). Defensibility is defined in such a way that incommensurable systems can be compared to each other using a single measure. The most defensible system would then receive the highest priority for defensive resources.

We compute the measure outlined above for several representative data sets, including property losses data from Willis [3] and air transportation data from the US Department of Transportation. We also derive rigorous results for an important class of problems involving discrete assets of differing values, such as airports, military bases, or commercial buildings. Among our more surprising findings is that some types of systems may be more defensible against deliberate attackers than against random hazards.

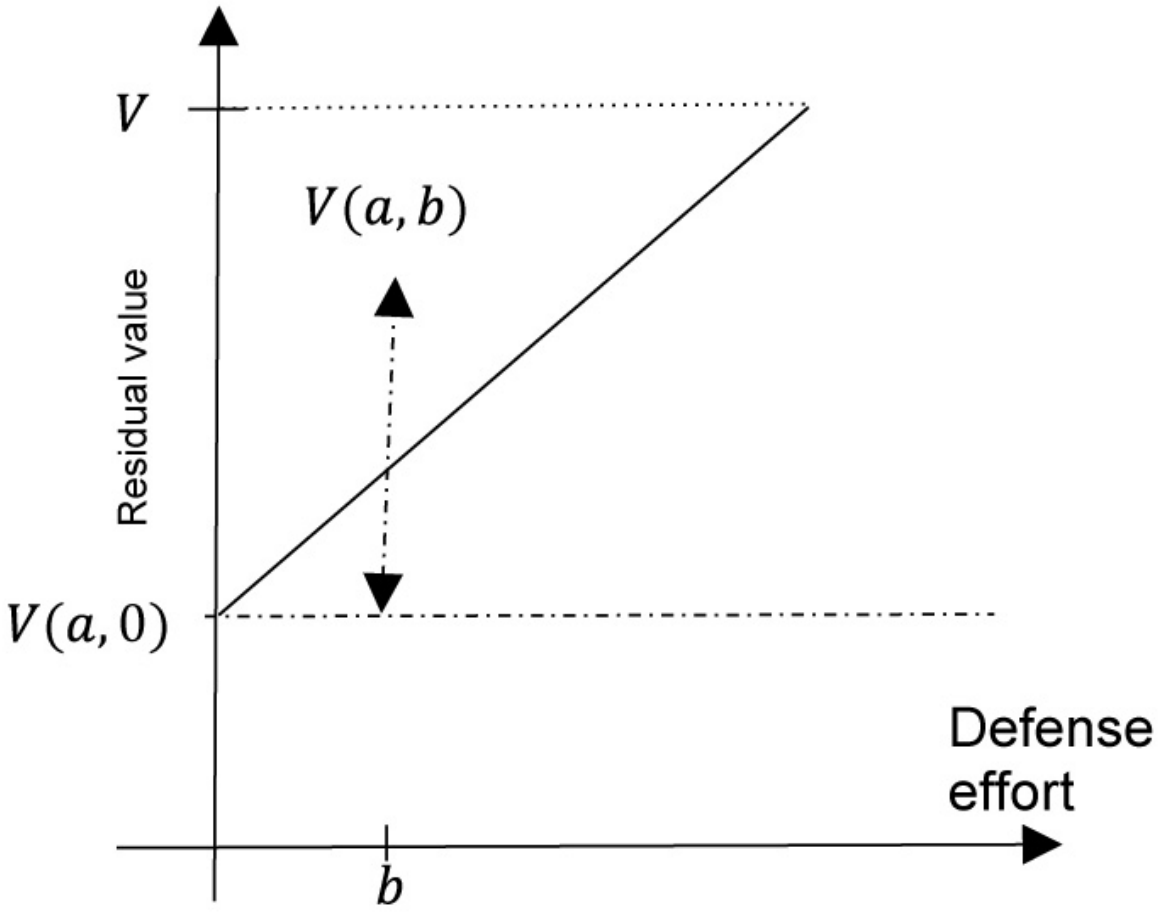

Fig. 1. Hypothetical curves showing the residual values of three systems with different defensibilities. and are, respectively, the residual values of the system after an attack effort in the case of zero defense effort and effort , respectively. The upper (concave) curve represents a highly defensible system, where a small defense effort results in a large increase in the residual value of the system. Its defensibility at the point *b* is indicated by the vertical arrow between the upper curve *V(a, b)* and the dashed line *V(a, 0).*

To summarize, security analysis to date has been focused on existing notions such as vulnerability and resilience. Our analysis here is based on the observation that some at-risk systems may be much easier to improve than others. We argue that risk analysts and managers would benefit by considering defensibility in their risk management plans.

About the Authors

Prof. Vicki Bier, PhD. Department of Industrial and Systems Engineering, University of Wisconsin-Madison, 1513 University Avenue, Madison, WI, 53706 USA bier@engr.wisc.edu

Prof. Alexander Gutfraind, PhD. Uptake Technologies, Inc, 60654, Chicago, IL and Laboratory for Mathematical Analysis of Complexity and Conflicts Loyola University Medical Center, Maywood, IL, 60153 USA agutfraind.research@gmail.com

Mr. Ziyang Lu. Department of Industrial and Systems Engineering, University of Wisconsin-

Madison, 1513 University Avenue, Madison, WI, 53706 USA zlu55@wisc.edu

Bibliography

[1] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, and K. R. Wierzbicki, “Methodology for identifying near-optimal interdiction strategies for a power transmission system,” *Reliab. Eng. Syst. Saf.*, vol. 92, no. 9, pp. 1155–1161, Sep. 2007.

[2] V. M. Bier and A. Gutfraind, “Risk analysis beyond vulnerability and resilience – characterizing the defensibility of systems and targets,” *Risk Anal.*, under revision 2017.

[3] H. H. Willis, “Guiding Resource Allocations Based on Terrorism Risk,” *Risk Anal.*, vol. 27, no. 3, pp. 597–606, Jun. 2007.