SUMMARY

As information systems become increasingly important to the functions of organizations, security and reliable operation of these systems are also becoming increasingly important. Interoperability, information sharing, collaboration, design imperfections, limitations, and the like lead to vulnerabilities that can endanger information system security and operation. Unfortunately, understanding an organization's reliance on information systems, the vulnerabilities of these systems, and how to mitigate the vulnerabilities has been a daunting challenge, especially for less well-known or even unknown vulnerabilities that do not have a history of being exploited.

RAND has developed and evolved a methodology to help an analyst understand these relationships, facilitate the identification or discovery of system vulnerabilities, and suggest relevant mitigation techniques. This Vulnerability Assessment and Mitigation (VAM) methodology builds on earlier work by Anderson et al. (1999) and fills a much-needed gap in existing approaches by guiding a comprehensive review of vulnerabilities across all aspects of information systems (including not only cyber objects but also physical, human/social, and infrastructure objects[1]) and mapping the vulnerabilities to specific security techniques that can address them.

The VAM methodology takes a top-down approach and seeks to uncover not only vulnerabilities that are known and exploited or revealed today but also the vulnerabilities that exist yet have not been exploited or encountered during operation. Thus, the methodology helps to protect against future threats or system failures while mitigating current and past threats and weaknesses. Also, sophisticated adversaries are always searching for new ways to attack unprotected resources (the "soft underbelly" of the information systems). Thus, the methodology can be valuable as a way to hedge and balance both current and future threats. Also, the complexity of information systems, and their increasing integration with organizational functions, requires additional considerations to ensure that design or architectural weaknesses are mitigated.

[1]An "object" is any part of the system that contributes to the function, execution, or management of the system. The partitioning of information system components into conceptual "objects" facilitates the consideration of components that can otherwise be neglected in security assessments (i.e., security breaches can arise from weaknesses in physical security, human limits and behavior, social engineering, or compromised infrastructure in addition to the more publicized compromises, such as network attacks). It also allows the separation of vulnerability attributes from the system component that may have that attribute.

MAPPING SECURITY NEEDS TO CRITICAL ORGANIZATIONAL FUNCTIONS

The methodology employs the following six steps:

1. Identify your organization's essential information *functions*.
2. Identify essential information *systems* that implement these functions.
3. Identify *vulnerabilities* of these systems.
4. Identify pertinent *security techniques* to mitigate these vulnerabilities.
5. *Select and apply* techniques based on constraints, costs, and benefits.
6. *Test* for robustness and actual feasibilities under threat.

   Repeat steps 3–6 as needed.

The methodology's guiding principles are the links back through critical systems to important organizational functions as well as assessments of the appropriateness of security techniques in each specific situation. This approach not only guides the evaluator through the myriad possible security techniques selections but also provides management rigor, prioritization, and justification for the resources needed, helping others to understand what needs to be done and why.

IDENTIFYING WELL-KNOWN AND NEW VULNERABILITIES

Vulnerabilities arise from the fundamental properties of objects. The VAM methodology exploits this fact to provide a relatively comprehensive taxonomy of properties across all object types, leading the evaluator through the taxonomy by using a table of properties applied to *physical*, *cyber*, *human/social*, and *infrastructure* objects (see Table S.1). This approach helps the evaluator avoid merely listing the standard, well-known vulnerabilities (a bottom-up, historical approach), but asks questions outside the range of vulnerabilities commonly identified. For example, vulnerabilities arise not only from such access points as holes in firewalls but also from such behavioral attributes as gullibilities or rigidities. These attributes may be exhibited by all types of system components: cyber, physical, human/social, or infrastructure.

IDENTIFYING AND DOWNSELECTING MITIGATIONS TO IMPLEMENT

The VAM methodology identifies a relatively comprehensive taxonomy of security technique categories to prevent, detect, and mitigate compromises and weaknesses in information systems (see Figure S.1). These techniques are grouped by techniques that improve system *resilience and robustness*; techniques that improve *intelligence, surveillance, and reconnaissance (ISR)* and *self-awareness*; techniques for *counterintelligence* and *denial of ISR and target acquisition*; and techniques for *deterrence and punishment*.

Table S.1

The Vulnerability Matrix

RAND*MR1601-tableS.1*

		Object of Vulnerability			
		Physical	Cyber	Human/Social	Enabling Infrastructure
	Attributes	Hardware (data storage, input/output, clients, servers), network and communications, locality	Software, data, information, knowledge	Staff, command, management, policies, procedures, training, authentication	Ship, building, power, water, air, environment
Design/Architecture	Singularity				
	Uniqueness				
	Centrality				
	Homogeneity				
	Separability				
	Logic/ implementation errors; fallibility				
	Design sensitivity/ fragility/limits/ finiteness				
	Unrecoverability				
Behavior	Behavioral sensitivity/ fragility				
	Malevolence				
	Rigidity				
	Malleability				
	Gullibility/ deceivability/naiveté				
	Complacency				
	Corruptibility/ controllability				
General	Accessible/ detectable/ identifiable/ transparent/ interceptable				
	Hard to manage or control				
	Self unawareness and unpredictability				
	Predictability				

The methodology uses multiple approaches to identify which security techniques should be considered to address the identified vulnerabilities.

First, a matrix maps each vulnerability to security techniques that are either primary or secondary candidates for mitigating the vulnerability. The matrix also cautions when security techniques can incur additional vulnerabilities when they are implemented (see Figures S.2 and S.3). Finally, the matrix notes the cases in which vulnerabilities actually facilitate security techniques, thus resulting in a beneficial side effect.

Second, users will come to this methodology with different intents, responsibilities, and authorities. The methodology reflects this fact by filtering candidate security techniques based on the evaluator's primary job role—operational, development, or policy. The methodology also partitions information system compromises into the fundamental components of an attack or failure: knowledge, access, target vulnerability, non-retribution, and assessment. *Knowledge* of the target system is needed to design and implement the attack. *Access* is needed to collect knowledge and execute an attack on the target vulnerability. Without the core *target vulnerability*, no attack is possible in the first place. *Non-retribution* (or even its first component of non-attribution) is needed to minimize backlash from the operation. Finally, *assessment* of an attack's success is critical when other operations rely on the success of the attack. In the case of a nondeliberate system failure, only the target vulnerability that enables the failure is the critical component.

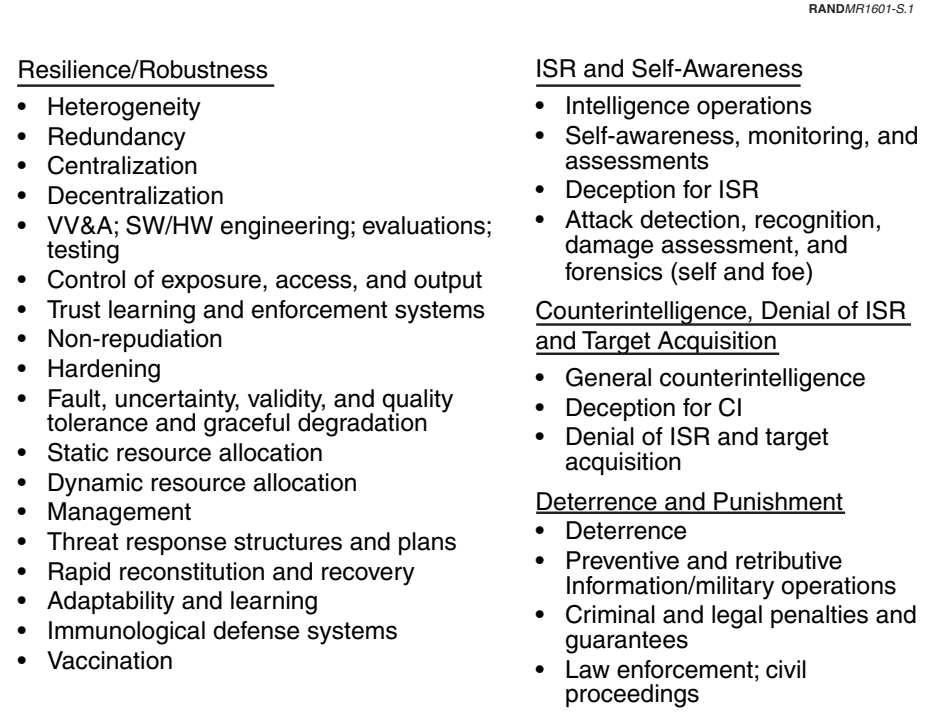

Figure S.1—Security Mitigation Techniques

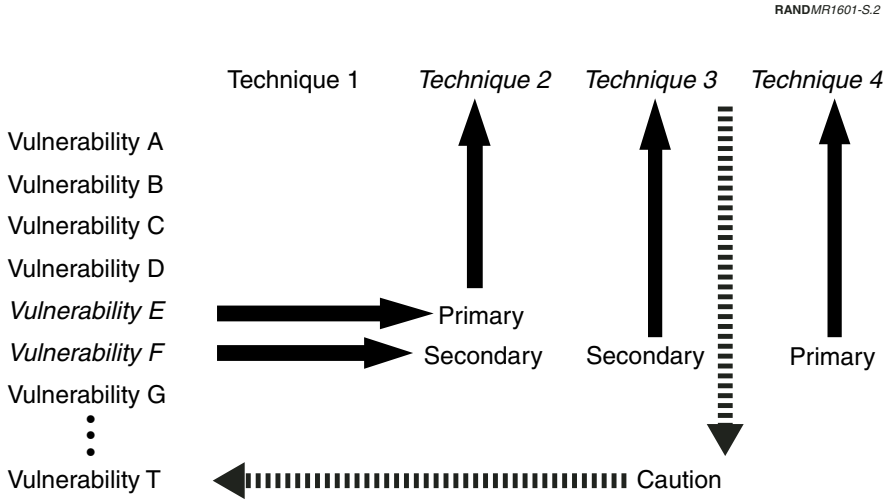

Figure S.2—The Concept of Mapping Vulnerabilities to Security Mitigation Techniques

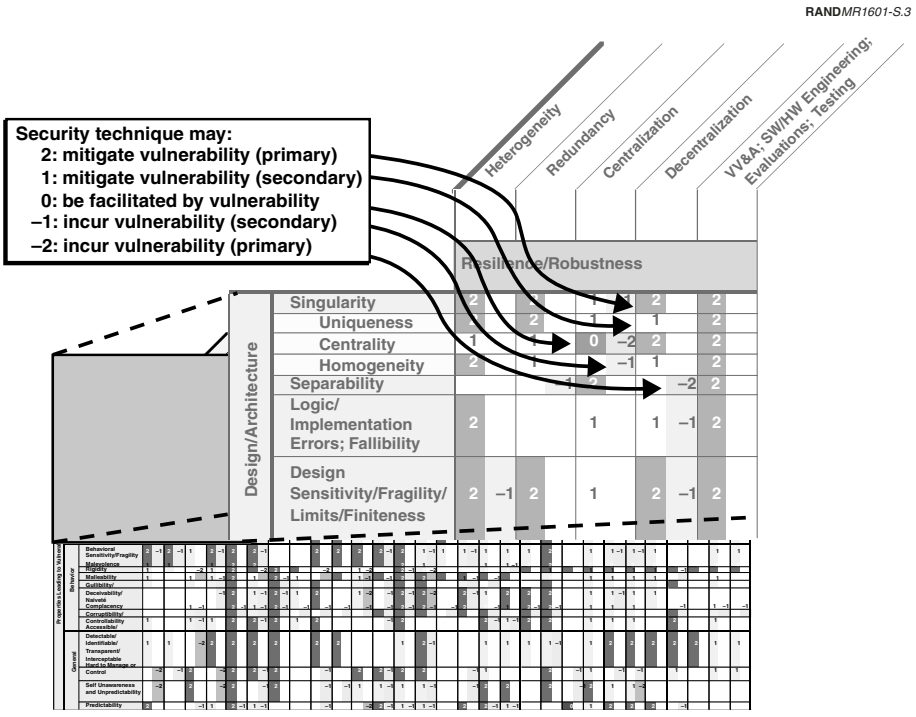

Figure S.3—Values Relating Vulnerabilities to Security Techniques

In addition to filtering the techniques further, this partitioning exploits the important observation that, in attacks, denial of a critical component of an attack can prevent an attack without necessarily addressing the fundamental target vulnerability. The partitioning also suggests additional options for evaluators, based on their situation and job role. For example, operational users cannot redesign the architecture of an information system developed by others, but they can often limit knowledge and access to the system.

AN AUTOMATED AID IN USING THE VAM METHODOLOGY

Finally, an automated prototype tool implemented as an Excel spreadsheet greatly improves the usability of the methodology. The tool guides the evaluator through assessment of vulnerabilities, evaluation of risks, review of cautions and barriers to security techniques, selection of techniques to implement, and estimation of the risks after implementation. Figure S.4 shows the part of the tool where the evaluator specifies his or her job role, and the risks are rated across all five attack components. Readers may obtain a copy of this prototype online at www.rand.org/publications/MR/MR1601/.

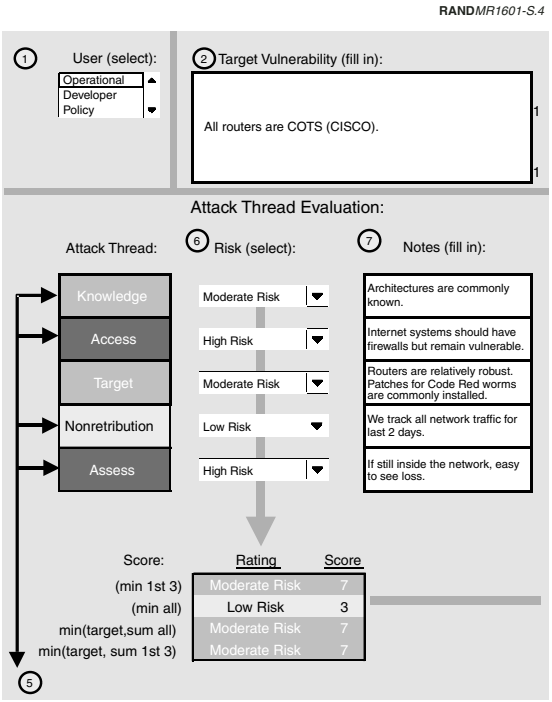

Figure S.4—User and Attack Component Filtering in the VAM Tool (notional values)

CONCLUSIONS

The VAM methodology provides a relatively comprehensive, top-down approach to information system security with its novel assessment and recommendation-generating matrix and filtering methods.

The vulnerabilities and security taxonomies are fairly complete. Viewing vulnerability properties separate from system objects has proved to be a valuable way of reviewing the system for vulnerabilities, since the properties often apply to each type of object. Also, each object type plays an important role in the information systems. The realization and expansion of the vulnerability review to explicitly consider physical, human/social, and infrastructure objects, in addition to cyber and computer hardware objects, recognize and accommodate the importance of all these aspects of information systems to the proper function of these systems.

VAM fills a gap in existing methodologies by providing explicit guidance on finding system vulnerabilities and suggesting relevant mitigations. Filters based on vulnerabilities, evaluator type, and attack component help to improve the usability of the recommendations provided by the methodology.

Providing a computerized aid that executes the methodology during an evaluation greatly improves the usability of the methodology, especially because the current approach generates many more suggestions than the earlier version in Anderson et al. (1999). The current spreadsheet implementation in Excel has the benefit of being usable by the large number of personal computer users who already have the Excel program on their machines. The spreadsheet also gives the user the flexibility to generate analysis reports and even input custom rating algorithms to accommodate local needs and situations.

The methodology should be useful for both individuals and teams. Individuals can focus on their specific situation and areas of responsibility, while teams can bring multiple kinds of expertise to bear on the analyses, as well as perspectives on different divisions within an organization. The methodology also can be used in parallel by different divisions to focus on their own vulnerabilities and can be integrated later at a high-level review once each group's justifications and mappings back to the organization's functions are understood.