Proceedings of the 2006 Symposium
39th Hawaii International Conference on System Sciences

Adding the Fourth "R": A Systems Approach to Solving the Hacker's Arms Race

Barbara Endicott-Popovsky and Deb Frincke, *IEEE Member*

In this paper, the authors propose a modification of CERT's 3 R model to include a 4th R, the discipline of Redress, identified as a necessary step to end the hacker arms race. Redress will require implementation of computer forensic investigation methods, tools and techniques that will permit evidence gathered to be admissible in a court of law, a standard not often understood or followed by many who are responsible for securing networks today. This leads the authors to conclude that there is a need for future work that will involve re-examination of the mechanisms and procedures used to collect evidence of network intrusions in order to ensure that the Rules of Evidence requirements are considered.

I. Introduction

Intuitively, we're in what could be described as an "arms race" with the hacker community. As our information system defenses get better, hackers' skills must get better if they want to continue to wage successful attacks. As their skills get better, we must improve our defenses to make our systems more secure if we want to repulse their attacks. This only serves to inspire hackers to acquire even better skills and abilities, which then stimulates us to improve the security of our systems even more, and so on, in a never-ending pattern of escalation with no obvious way out. (Figure 1) Applying a systems approach, we propose strategies for disrupting this cycle.

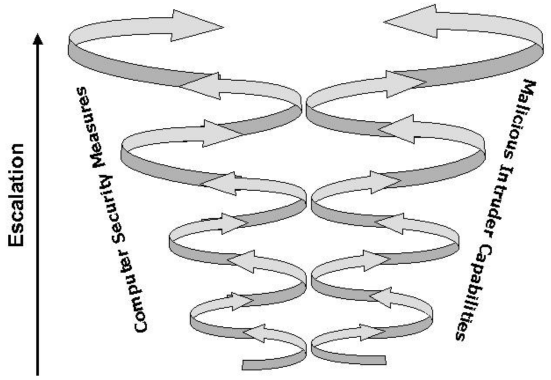

Figure 1 The escalation tendency of the hacker arms race

Barbara Endicott-Popovsky, Associate Director for the Center for Information Assurance and Cyber security and SeniorLecturer, University of Washington;
Deb Frincke, Ph.D., Chief Scientist Cybersecurity, Pacific Northwest National Laboratory and Associate Professor (on leave), Computer Science Department, University of Idaho

II. Accelerating factors

Several trends coincide with this escalation cycle, amplifying its effects. At the same time, our organizations are becoming increasingly reliant on public networks, often without tempering enthusiasm with a concern for security. [1] These trends create a lethal "accelerant" for the hacker arms race.

A. Increasingly sophisticated hacker tools

With the advance of technology, it now takes less technical knowledge to launch increasingly sophisticated attacks using increasingly sophisticated hacker tools, fueling the escalation cycle. This is an open invitation to those inclined toward online mischief.

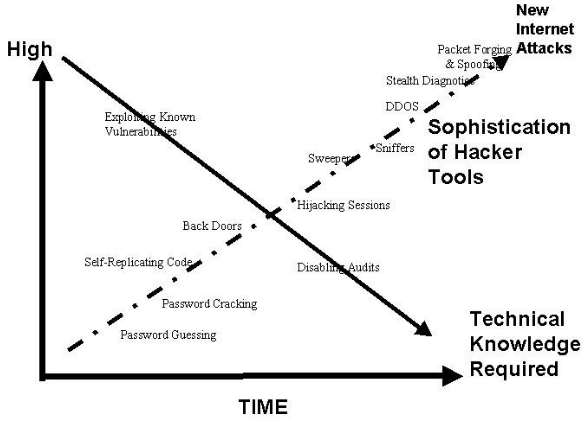

Figure 2. Hacker threat capabilities
Source: TriGeo Network Security Presentation 9/23/02[2]

B. Increasing volume of attacks

The CERT Coordination Center[1] for the Carnegie-Mellon Software Engineering Institute reports the following regarding their experiences with cyber attacks reported from 1998 through 2003 (Table 1). [3] (By 2004, use of

[1] CERT (Computer Emergency Response Team) gathers credible statistical data about the Internet security experiences of its members and sponsors, who include government, academia, industry, security experts, law enforcement and vendors.

widespread automated attack tools made tracking numbers of incidents of little value.)

Table 1 Recent CERT/CC Experiences

	1998	**1999**	**2000**	**2001**	**2002**	**2003**
ReportedIncidents CERT	3734	9859	21,756	52,658	82,094	137,529
Vulnerabilities Reported	262	417	1,090	2,437	4,129	3,784
PublishedVulnerability Notes	8	3	47	326	375	255

Source: Carnegie-Mellon CERT [3]

The cumulative curve below, derived from data in Table 1–first row, depicts the significant increases in incidents reported to CERT during this same period. (Figure 3).

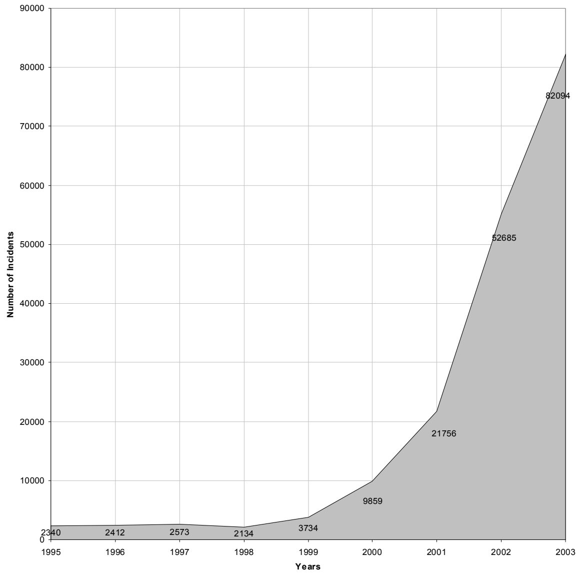

Figure 3. Cumulative CERT incidents 1995- 2003

With these increases in the rise in incidents, one might ask why the situation continues unabated. The 2004 CSI-FBI 9th Annual Computer Crime and Security Survey reports that organizations continue to increase their investments in tools and techniques designed to block computer attacks and protect computer and information systems. [4] Why, then, have these not been sufficient to stop the continued escalation of the hacker arms race?

III. APPLYING GENERAL SYSTEMS THEORY

The authors believe that insight into this problem may be gained by applying systems analysis, defined as the 'transdisciplinary study of the abstract organization of phenomena, independent of their substance, type, or spatial or temporal scale of existence." [5] As a field of study, general systems theory emerged in the 1930's led by such luminaries as Russell Ackoff and Ludwig von Bertalanffy. It "investigates both the principles common to all complex entities, and the (usually mathematical) models, which can be used to describe them." [5]

A complex set of factors keeps the escalating hacker arms race in place, in spite of the frustration and pain that it causes victims. By applying systems analysis, a recommended approach for solving complex problems [5, 6], a way can be discovered to intervene in the hacker arms race and disrupt the escalating spiral.

In the balance of this paper, the hacker arms race is analyzed by applying general systems theory in order to discover an exit to this self-reinforcing system.

IV.

A system is defined as "a collection of parts, which interact with each other to function as a whole." [8] Systems have common characteristics. All systems require energy to run and maintain. They are self-perpetuating and stable--resistant to change. [8] Using the above definition, the hacker arms race behaves as a system. It is explained below.

A. Describing the hacker arms race system

Attackers and targets can be viewed as behaving as components in a system, locked in a pattern of escalating behavior in response to one another. Using the language of systems, a system can be described schematically using a simple drawing, called an archetype, which identifies system components and the feedback loops holding them together in relationship to one another. An archetype explains the dynamics of a system, i.e., how the system functions. [5, 8]

Senge has identified a small finite number of these archetypes, which, either singly or in combination, are sufficient to describe behavior in all systems, whether it be the human body, an organization, or a computer system. Discovery of which archetype applies in any one situation is a process of discovery by analogy using an inductive reasoning approach. [6]

By induction, the hacker's arms race, is best described by the escalation archetype (Figure 4).

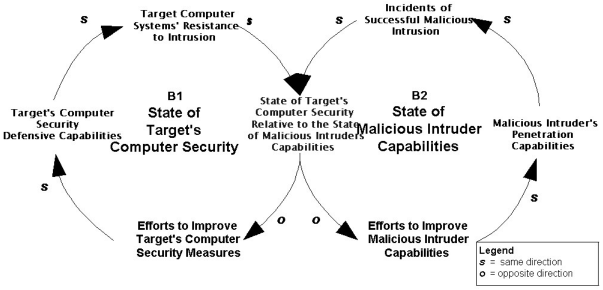
Target Computer Systems' Resistance to Intrusion
Incidents of Successful Malicious Intrusion
s
s
s
s
B1
State of Target's Computer Security
Target's Computer Security Defensive Capabilities
State of Target's Computer Security Relative to the State of Malicious Intruders Capabilities
B2
State of Malicious Intruder Capabilities
Malicious Intruder's Penetration Capabilities
s
s
o
o
Efforts to Improve Target's Computer Security Measures
Efforts to Improve Malicious Intruder Capabilities
Legend
s = same direction
o = opposite direction

Figure 4 Escalation archetype applied to the hacker arms race system

In this instance, the escalation archetype reflects an environment where the state of a target's computer security depends on the state of malicious intruder capabilities. The loop on the left represents the state of a target's computer security, indicating the activities and results that will transition that state from more to less secure, and back again. The loop on the right represents the state of malicious intruder capabilities, indicating the activities and results that will transition that state from more to less capable, and back again. In the language of systems, both loops are negative feedback loops or balancing loops, labeled B1 and B2, meaning these two respective systems self-regulate, like a thermostat. Putting them together, they regulate against each other.

The model can be read beginning with the text in the middle. This is the initiating energy that provides system momentum. Then follow the direction of both arrows, simultaneously, using the legend where *S* indicates action in the same direction and *O* indicates action in the opposite direction. The model then reads:

> As the **state of a target's computer security** rises above the **state of malicious intruder capabilities** then two things happen: 1) **efforts to improve the target's security measures** decrease, in other words complacency sets in for B1 and 2) **efforts to improve malicious intruder capabilities** increase, in other words the intruders fight back to gain ascendancy. Continuing along B1, as **efforts to improve the target's security measures** decrease, the **target's computer security defensive capabilities** decrease (movement in the same direction) and the **target computer systems resistance to intrusion** likewise decreases. Continuing along B2, as efforts to improve **malicious intruder capabilities** increase, **malicious intruder penetration capabilities** increase (movement in the same direction) and incidents of successful malicious intrusion likewise increase. Now the **state of malicious intruder capabilities** rises relative to the **state of the target's computer security**. The hackers now are able to overcome the security measures protecting the target's systems.
>
> As the **state of malicious intruder capabilities** increases relative to the **state of the target's computer security**, then, again, two things happen: 1) **efforts to improve the target's security measures** increase, in other words the computer security professionals fight back to gain ascendancy and 2) **efforts to improve malicious intruder capabilities** decrease, in other words the intruders now become complacent. Continuing along B1, as **efforts to improve the target's security measures** increase, the **target's computer security**

defensive capabilities increase (movement in the same direction) and the **target computer systems' resistance to intrusion** likewise increases. Continuing along B2, as **efforts to improve malicious intruder capabilities** decrease, **malicious intruder penetration capabilities** decrease (movement in the same direction) and **incidents of successful malicious intrusion** likewise decrease. Now the **state of the target's computer security** rises relative to the **state of malicious intruder capabilities**. The target's computer security is better able to resist the malicious intruder.

When the **state of the target's computer security** rises relative to the **state of malicious intruder capabilities**, the cycle repeats, and so on, indefinitely, in an endless process of escalation.

B. Resolving the hacker arms race system

All systems have vulnerabilities: built-in delays that make them "wobble," reaction time limits, and limits to the amount of change they can endure before collapsing. According to systems theory, rather than directly "attacking" a system, it is much better to analyze the way components are arranged first, looking for vulnerabilities, then to change the way the pieces interact. [6, 9]

Thus, to exit the hacker's arms race, the system must be examined as a whole its components identified, how the components interact discovered, and the system's vulnerabilities exposed. This approach leads to solutions for resolving any system, resulting in lasting change. [2]

Using the escalation archetype to analyze the system and identify potential vulnerabilities, focus is turned to the right side of the escalation model, the intruder's side, where the energy fueling this system originates. Targets behave in response to the intruders. One might postulate that if the intruders were to quit, targets would not be as energized to continually improve the security of their systems. [3]

C. Applying a mathematical model

The following mathematical model provides another way to analyze the hacker arms race. The model attempts to describe hacker behavior (irrespective of capability), and is derived from work by H.R. Varian within the School of Information Management at UC Berkeley. It identifies components that comprise hacker motivation and the mathematical relationships among them. Examination gives insight into possible interventions that could lead to disruption of the hacker arms race. [16] [4]

Equation 1:
$M = f\ [\ P\ (v)\ -\ (c_1 + c_2\ )]$

where:

M = Hacker motivation
P = the probability of not failing to intrude
v = the value of success to the hacker
c_1 = the cost to the hacker
c_2 = the consequences to the hacker

According to this model, hacker motivation is a function of the *probability of not failing to intrude* (P), multiplied by the *value of success to the hacker (v)*, less the sum of the *costs and consequences to the hacker* ($c_1 + c_2$). Applied to the current situation, with the *probability of not failing to intrude* high (given the easy accessibility of targets) [17] and with the value of success prized by the hacker, according to Varian's model, P and v amplify the effects of each other. Additionally, with *costs and consequences to the hacker* low, referring back to the information found in Table 2, there is little to deter motivation to indulge in malicious online behavior.

Inspecting this expression, to change the outcome, either P, the *probability of not failing, to intrude*, can be lowered or *costs and consequences to the hacker*, represented by ($c_1 + c_2$), can be increased.

Previous security measures have focused on lowering P by increasing defensive measures protecting systems. The previous systems analysis indicated that this appears to have led to a never-ending hacker arms race. Raising the value of ($c_1 + c_2$) is an alternative strategy.

[2] In other words, when basic alterations take place within a system, impacting the way its components interact, any change, no matter how small, will create a permanent change to the system. Likewise, no matter how hard one pushes directly at a system, if no effort is made to change the way components interact, any change will only be temporary. The system will rebound eventually to its original state.

[3] Experience appears to bear out this assumption: organizations do not like to spend money on security if it is not necessary. [10]

[4] This model is outlined in a presentation entitled the "*PBIs on Economics of Computer Security*." [16]

D. Analyzing the model

Since intruder behavior has been identified as the starting point or "engine" in this system, some means to inhibit intruder motivation (*M*) must be identified. In Table 2 the conditions and characteristics of targets and intruders are examined to identify components that might be leveraged to change the hacker arms race system.

Table 2 Conditions characterizing targets vs. intruders

	Time	**Costs**	**Consequences**
Targets	Open-ended	Open-ended	Open-ended
Intruders	At their discretion	Nominal	None

Interpreting Table 2, targets have an open-ended vulnerability in terms of the time and money they must invest to recover from attacks, while intruders can spend time at their discretion and incur only nominal expenses.[5]

Targets also have an open-ended responsibility to recover from attacks, while intruders suffer virtually no accountability for their actions. Due to the anonymity that hackers can adopt in public networks, few are caught, and fewer still are ever prosecuted. [11, 12, 13, 14, 15] The penalties for those who are caught are very minor compared to the damage they cause. [11, 12, 13, 14, 15]

Thus, this system appears to benefit hackers at the expense of targets, resulting in an uneven playing field,[6] essentially giving hackers control of the system. They control the time they spend attacking targets and the tools and exploits they employ. In a sense, it is their discretion how much time and money targets are forced to spend on recovery. Hackers suffer few consequences for their actions and remain, for the most part, undetected.

As long as targets remain in a defensive posture, focusing on surviving attacks deemed inevitable, they remain accountable for the outcomes of the hackers arms race. Figure 5 illustrates the inequality in accountability that this situation poses.

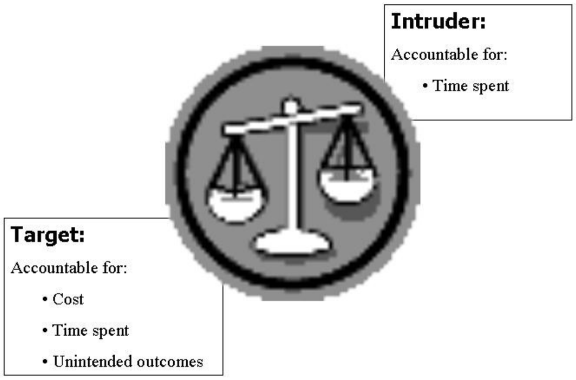

Figure 5. Target vs. intruder: the inequality of accountability

In practice, targets have tolerated this inequality, recovering systems and patching as intrusions have occurred, absorbing the consequences of intruder attacks. As the impacts of cyber attacks grow in consequence, this becomes an increasingly intolerable situation. [14, 15]

E. Increasing costs to the hacker

To increase the *costs and consequences* to an attacker for intruding behavior, targets have a number of options available. For example, a target might adopt a policy of attacking back (active defense) designed to disable or "crash" an attacker's system; rendering the attacker harmless for some period of time. The problem with an active defense strategy is unleashing unintended consequences, and legal liability, arising from being linked to public networks. [18, 19, 20]

This makes active defense an undesirable remedy–for now.[7] Thus for the purposes of this paper, it will not be considered a viable choice for intervening with the arms race escalation cycle.

As an alternative, targets might incorporate strategies that increase consequences for intruding by identifying the attackers and holding them accountable. Given the profile of hackers [21, 22, 23], this might be the best choice for intervening with the hacker arms race system.[8]

[5] Since the hacker community generously shares the tools of their trade, hackers only need Internet access and a PC to be in business. Both are relatively inexpensive.

[6] It is difficult to trace intruders from attack to source. Intruders can disguise themselves through "anonymizers" or stepping stones, and ISP's don't keep records for long periods of time, making identifying intruders difficult.

[7] *Active defense*, attacking back, is under discussion by some practitioners as a possible alternative for ending the hacker arms race. The legal ramifications and unintended consequences have deterred adoption of this approach for now. [18, 19, 20]

[8] While psychologists don't entirely agree on a profile of the average hacker, most believe they are typically white males between the ages of 15 and 35 without much social life and with a lot of time on their hands. [23] Anonymity is comfortable for them; they tend to be quite introverted.

F. Toward a candidate for intervention

Reviewing the elements of Table 3, intruder **Costs** (c_1) are nominal while intruder **Consequences** are none (c_2). Deploying defensive measures such as firewalls and intrusion detection systems, current target defensive strategies have focused on increasing the time penalty, or **Costs** (c_1), to hackers.

Hacker response to these actions has been either to try the next target (there are plenty available!) or develop better skills. Continuing these strategies appears to continue to fuel the hacker arms race. Since active defense strategies are ruled out as well, increasing **Costs** (c_1) does not appear to be an immediate candidate for intervention.

Examining **Consequences** (c_2) as a potential candidate remains.

Table 3 Identifying a candidate for intervention

	Time	**Costs** (c_1)	**Consequences** (c_2).
Targets	Open-ended	Open-ended	Open-ended
Intruders	At their discretion	Nominal	**None**

G. Intervening from outside the system

Developing strategies that focus on increasing consequences to the intruder for hacking behavior (c_2) from "None" to something more significant is suggested. Increased consequences can be introduced from outside the hacker arms race through intervention from the legal system.
This is supported by general systems theory,[9] which suggests that the solution to any system problem is outside the system itself. [5, 6] Thus, in order to disrupt never-ending escalation, an outside intervention must take place that blocks the energy fueling the system, thus limiting its growth.

If the goal is to disrupt the escalation cycle, by introducing legal consequences (c_2) to the hacker, using the previously described mathematical model, hacker motivation will decrease and the disparities between hackers and targets should begin to come into balance. (Figure 6)

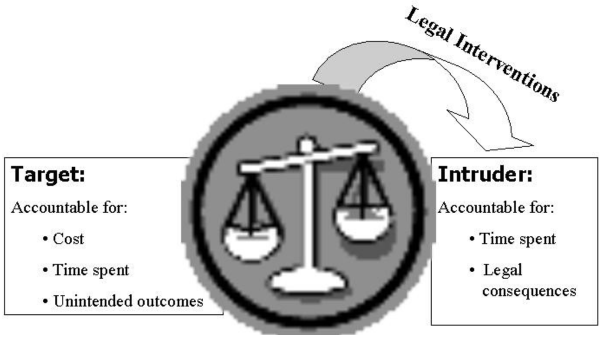

Figure 6 Leveling the playing field

H. Why legal intervention has been limited

Holding criminals accountable through the legal system is not a new idea. The criminal justice system is based on the concept that consequences for criminal behavior are an effective deterrent.

The question then arises 'why haven't targets changed their focus from increasing costs in terms of time a hacker spends breaking into a system to a focus on holding them legally accountable?'

The answer is that when targets do pursue either civil or criminal prosecution, the guilty parties are often found 'not guilty,' or punishments are small. [10, 11, 12, 13, 14, 15] This lack of success has made the effort to track down and convict hackers not a cost effective choice for targets.

Further, there are other inhibitors, like the fear of negative publicity and the concern that needed operational personnel and equipment will be consumed with non-productive activities, etc. [4, 13, 14, 15]

In addition, there may be another reason associated with the behavior of systems--the inertia inherent in all systems.[10] As a system, the hacker's arms race is resistant to change. It is held in place by the current context previously examined. This includes the mindsets of both

Further, according to psychologists, intruders find encouragement in their anonymity. They seek the thrill and sense of power they gain from mastering technology and causing major disruptions without being caught. [21, 22, 23] Increasing accountability for their actions would remove this reward.

[9] This recommendation is also supported by various theories of law enforcement that suggest consequences are effective deterrents. [14]

[10] Systems have a tendency to return to their original structure unless components are altered in some permanent way. They are said to be self-sustaining. [6, 7, 8, 9]

hackers and targets. Hackers are motivated to pursue targets as long as costs and consequences are insignificant and targets have continued to assume a defensive, reactive strategy in response.

Several practitioner models for 'operationalizing' security confirm the target mindset and appear to institutionalize the current hacker arms race system. One model will be addressed that specifically describes security strategies that targets can adopt to protect their systems. A change to this model will be suggested that is directed at altering the target mindset, thus permanently changing the balance in the arms race.

I. Institutionalization of the unending escalation in the hacker arms race

A never-ending, escalating computer security arms race is reflected in the emerging discipline of survivability, defined as the "ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures and accidents." CERT researchers, Ellison, et. al., state that the discipline of survivability "can help ensure that systems can deliver essential services and maintain essential properties including integrity, confidentiality, and performance despite the presence of intrusions." [24]

While previous point solutions--such as "PKIs, VPN's and firewalls"--focused on blocking attacks, the survivability approach reflects the inevitability of experiencing attacks [24, 25], suggesting there is no resolution to the hacker arms race. In a paper introducing and applying the survivability model, the authors assert that "...Despite the best efforts of security practitioners, no amount of hardening can assure that a system connected to an unbounded network [such as the Internet] will be invulnerable to attack." [24]

The 3R model for survivable systems is at the heart of the survivability discipline. Examining its elements demonstrates the mindset of the inevitability of attacks that appears to dominate current practice.

J. The 3R model of survivability

The survivability discipline is captured in the CERT 3 R model,[11] for defining survivability strategies devised to secure computer systems. [25] The 3R's—resistance, recognition, and recovery—are defined in Table 4. Note that all three strategies reflect the inevitability of attacks.

Table 4 Strategies of survivable systems

Survivability Strategy	**Tools**
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react or adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • Replication • Backup systems • Fault tolerant designs

Source: Ellison, et.al. [25]

Implicit in the survivability model is the assumption that the continual escalation of the hacker arms race is a given. It's not a matter of "if attacks will occur," but "when."

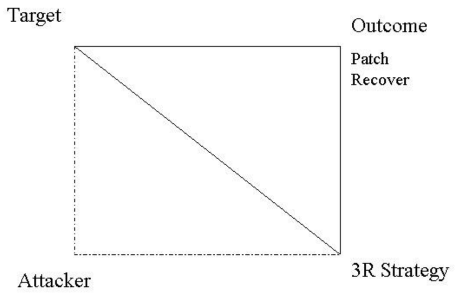

Figure 7 Employing a 3R strategy

Employing a 3R strategy, the outcome following an attack is patch and recover. Identifying the attacker is not a primary concern. (Figure 7) The idea of holding the offender accountable is not a major concern. Restoring system function is.

The authors contend that this mindset of the inevitability of attacks keeps targets in a never-ending arms race with attackers. The addition of another strategy is called for, one designed to prevent attacks at the source--the attacker--by modifying his/her behavior, thus disrupting the tendency of the arms race.

[11] Later a fourth strategy, **adaptability/evolution**, was added by CERT researchers. For this paper, we will examine the 3R model. [26]

K. "Adding the 4th R

To change intruder behavior by increasing consequences to the intruder, the fact that few organizations pursue legal action must be addressed. To begin, this necessitates a change in policy that would incorporate among an organization's computer security strategies a willingness to go to court and the ability to prevail.

To formalize this change in strategies, the authors propose that the 3R model be modified by the addition of a 4th R–**Redress** [27], defined as the ability to hold intruders accountable. Initially **Redress** will be accomplished by pursuing accountability for intruder behavior in the legal system. When the issues surrounding the legal and ethical implications of active defense are resolved, then **Redress** could also include the ability to retaliate when attacked. Both are included in the revised model. For the balance of this discussion, attention will focus on legal remedies as the primary vehicle for **Redress**.

L. Redress defined

Redress will require incorporation of what Sommers calls computer Forensics, with a capital "F,"[12] in the security strategies of an adopting organization. [28] While computer forensics with a small "f" is assumed to be part of **Recovery**, this activity is usually not carried out in a rigorous enough fashion, suitable for admitting evidence in a courtroom.

The addition of this 4th R expands the duties of those responsible for securing networks to include adherence to the Rules of Evidence when investigating an intrusion. [13, 15, 28] This will likely require re-examination of current security policies, procedures, methods, mechanisms, and tools for compliance with more rigorous evidence collection and storage standards for courtroom admissibility.

The revised 4 R Model proposed by the authors is presented in Table 5. While, as mentioned previously, few hacking incidents have caused organizations to seek redress in a court of law, due to the many challenges of bringing a successful prosecution [13], it is expected that the appetite to seek legal remedy will grow as the severity of losses due to computer crime grows. [28] [13]

Table 5 Strategies of accountable systems

Survivability Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react or adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • Replication • Backup systems • Fault tolerant designs
Redress 1)Ability to hold intruders accountable in a court of law. 2)Ability to retaliate	• Computer Forensics • Legal remedies • Active defense

Employing a 4R strategy, the outcome following an attack is much different from the outcome when a 3R strategy is followed. Evidence is gathered and legal processes are pursued in addition to assuring system function is restored.

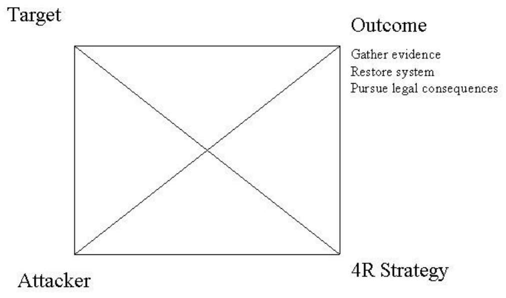

Figure 8 Employing a 4R strategy

[12] Sommers, a leading expert in digital forensics with the London School of Economics, makes the distinction between *computer forensics*, which is an investigatory activity to discover what happened prior to restoring computer systems that have been attacked, and *computer Forensics* with a capital "F" that implies the investigation is not only for discovering what happened, but also to determine who did it by using techniques for gathering and preserving evidence that will be upheld in a court of law.

[13] As evidence that this may now be occurring, there has been an increase in the number of incidents for which legal remedies are being pursued. [29] In addition, anecdotal evidence suggests organizations and the public are already experiencing losses that they no longer are willing to tolerate. [13, 14, 15, 28, 29]

Thus, identifying the attacker becomes a matter of concern. (Figure 8) There are additional implications to the arms race system, as well, that will be the subject of future investigations.

V. Indications for Future Work

The requirements for gathering evidence suitable for admissibility in a courtroom are much stricter than those needed for simply gathering evidence in order to restore a computer system to full function following an attack. [28] Since most practitioners follow a 3R strategic approach [29], the additional requirements related to collecting forensically sound evidence, arising from following a 4R strategy, are not widely understood or followed by systems administrators or those setting security policy or designing networks. [29] [14]

Future work will involve re-examination of Target and Attacker in the context of using a 4R strategy. It is expected that policies, procedures, methods, mechanisms, and tools currently employed by computer security professionals in a 3R environment will require modification in an environment where a 4R strategy is pursued. [29]

VI. Summary and Conclusions

This article has described and analyzed the hacker arms race system and current trends that accelerate the never-ending escalation cycle embodied in this system. The urgency to end the escalation was addressed through the application of techniques from systems analysis that identified vulnerabilities in the arms race system that could be leveraged to disrupt it.

Further analysis suggested that increasing consequences to intruders by holding them accountable in the legal system would be a better alternative to inhibiting the never-ending escalation of the hacker arms race than continuing to increase defenses which appears to only fuel the arms race. It was further suggested that this might require a change in mindset on the part of those targeted by attackers.

This change in mindset was formalized by adding a 4th R (Redress) to CERT's 3R model, which provides a new way of thinking about computer security countermeasures that would include instituting forensic approaches that adhere to the Rules of Evidence--something with which those responsible for securing networks are often unfamiliar.

Further, it was suggested that future work, proceeding along this avenue of inquiry, would involve re-examination of the policies, procedures, methods, mechanisms, and tools currently employed by computer security professionals in today's 3R environment to determine if they will require modification for an environment where a 4R strategy is pursued.

VII. References

[1] Oman, P., Schweitzer, E. and D. Frincke, "Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," Paper #4, *27th Annual Western Protective Relay Conference*, (Oct. 23-26, Spokane, WA), 2000.

[2] TriGeo (2002, September) *Network Security: Intrusion Detection System*. Presentation given at the Computer Forensics Workshop, University of Idaho, Moscow, ID.

[3] Carnegie-Mellon Software Engineering Institute CERT organization. (2003). *CERT/CC Overview*. Retrieved October 10, 2003 from the World Wide Web: http://www.cert.org

[4] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. CSI-FBI 9th Annual Computer Crime and Security Survey, 2004.

[5] Heylighen, F. and Joslyn, C (1992). Principia Cyberntica Web. Retrieved July 7, 2005, from the World Wide Web: http://pespmc1.vub.ac.be/SYSTHEOR.html

[6] Senge, P. M. (1990). *The fifth discipline.* New York: Doubleday Currency.

[7] Senge, P., Roberts, C., Ross, R.B., Smith, B.J.,& Kleiner, A. (1994). *The fifth discipline fieldbook: Strategies and tools for building a learning organization.* New York: Doubleday-Currency.

[8] Kim, D. H. (1992). *Systems archetypes I: Diagnosing systemic issues and designing high leverage interventions.* Waltham, MA: Pegasus Communications, Inc.

[14] For example, if the Rules of Evidence are not adhered to in the scramble to restore the system immediately upon an intrusion being detected, any information collected that might lead to a courtroom victory may be invalidated as to its admissibility. [13, 15, 28, 29]

[9] Umpleby, S.A. and E.B. Dent. (1998, September). *The Origins and Purposes of Several Traditions in Systems Theory and Cybernetics.* Paper Presented Cybernetics and Systems, George Washington University, Washington, D.C.

[10] Bailey, K. (2002, October 24). *The Risk Management Perspective on Security*. Presentation given at Computer Security and Cybercrime II: Legal Risks and Responsibilities in a Dangerous World Workshop, King County Bar Association, Seattle, WA.

[11] Mitnick, K. D. & Simon, W. L. (2002*). The Art of Deception*. New York: Wiley Publishing.

[12] Schneier, B. (2000). *Secrets and Lies : Digital Security in a Networked World.* New York: Wiley Publishing.

[13] Orton, I. (2002, October 24). *Coordinating with Law Enforcement on Security Issues*. Presentation given at Computer Security and Cybercrime II: Legal Risks and Responsibilities in a Dangerous World Workshop, King County Bar Association, Seattle, WA.

[14] Orton, I. (2003, Spring). *Guest Lecture: CSSE591 Computer Forensics*, Seattle University, Seattle, WA.

[15] Ryan, D. (2003, June). *New Directions in Cyber Law*. Paper Presented at the CISSE 7th Colloquiam. Washington, D.C.

[16] Varian, H.R. (1998, November 10). *The PBIs on Economics of Computer Security*. Presentation given at the School of Information Management, UC Berkeley, Berkeley, CA.

[17] Endicott-Popovsky, B.E., Fringke, D, “*Community Security Awareness Training*",” in Proceedings of the 6th Annual IEEE Information Assurance Workshop, June '05, USMA, West Point.

[18] Verry. J. (2003, August 19). *Hacking the hacker: How a consultant shut down a malicious user on a client's FTP server.* Retrieved from TechRepublic September 15, 2003 from the World Wide Web: http://techrepublic.com.com/5100-6329-5055990.html

[19] Jayawal, V., Yurcik, W., and David Doss. (No Date). *Internet hack back: Counter attacks as self-defense or vigilantism*? Retrieved September 15, 2003 from the World Wide Web: http://www.sosresearch.org/publications/ISTAS02/hackback.pdf

[20] Wright, B. (2001, September 25). *The legal risks of computer pests and hacker tools*. Retrieved September 15, 2003, from the World Wide Web: http://www.safersite.com/Whitepapers/LiabilityofPests.asp

[21] Rogers, M. (No Date) Retrieved August 5, 2003, from the World Wide Web: http://www.landfield.com/isn/mail-archive/1999/Jan/0087.html

[22] Hafner, K. and J. Markoff, J. (1995) *Cyberpunks: Outlaws and hackers on the computer frontier*.

[23] Frontline (Producer). (2001). *Hackers*. [Film]. PBS Video.

[24] Ellison, R.J., Mead, N.R., Longstaff, T.A. and R.C. Linger. (No Date) “*The Survivability Imperative: Protecting Critical Sustems*.” Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA. Retrieved October 10, 2003 from the World Wide Web: http://www.cert.org

[25] CERT Coodination Center. (no date). “*The Survivable Network Analysis Method: Assessing Survivability of Critical Systems*.” Presentation: Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. Retrieved October 10, 2003 from the World Wide Web: http://www.cert.org

[26] Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A. and. N.R. Mead. (May, 1999). “*Survivable Network Systems: An Emerging Discipline*.” CMU/SEI 97-TR-013, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA.

[27] Endicott-Popovsky, B and D. Frincke. (June, 2004). *Adding the 4th R*, 5th Annual IEEE Information Assurance Workshop Poster Session, West Point, New York.

[28] Sommers, P. (2002, September). *Emerging problems on digital evidence*. Presentation given at the Computer Forensics Workshop, University of Idaho, Moscow, ID.

[29] Dittrich, D. (Fall, 2003). *Info498 Introduction to computer security incident response*, University of Washington, Seattle, WA.