

Catch Me if You Can: A Taxonomically Structured Approach to Cybercrime

Lynne Yarbrow Williams, Department Head of Computer Science and Information Technology,
The University of New Mexico, Los Alamos

ABSTRACT

Computer crime can be problematic to define, owing to the complex variety of differing crimes involving computers and the rapid changes that advance and modify the underlying technology. The American Heritage® Dictionary Online (2000) defines computer crime as “criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data” (§ 1). If local access to the computer is considered as the sole entry vector for computer crime, this definition is adequate. With the pervasive incursion of networks and the Internet into modern society, thus making access to criminal activity using a computer located anywhere available to anyone from any location, the definition is acutely limited.

In reaction to cybercrime, there have been public and enterprise level attempts to attack cybercrime using a traditionally litigative approach to possible recourse strategies. Although current reports, such as the annual CSI/FBI Survey, reveal that enterprises are spending an average of three percent of their IT budget on information security, the combined categories of intrusions and unauthorized usage continue to increase. This poor level of performance seems to indicate that current strategies employed by organizations for the purpose of reducing or preventing intrusions and unauthorized usage have limited effectiveness or may be poorly applied. As global commerce and society in general becomes increasingly dependent on computer networks, the significance of attacks or disruption of those systems becomes elevated, as does the importance of effective investigation and deterrence of the attackers. Determining appropriate recourse strategies in regards to computer-network-related crime is increasingly crucial for any networked organization.

Introduction

Jurisdiction and physical presence of a perpetrator and evidence form the basis of the majority of existing legal structures that address criminal issues. Tangible, physical evidence is the foundation on which most successfully prosecuted crimes rest. Digital evidence obtained from a cybercrime intrusion is volatile, difficult to obtain or present in court, and requires a certain amount of adaptation in order to be acceptable to most courts. These difficulties of application may be illustrated in more detail by examining specific comparisons of cybercrime incidents to existing laws, as well as procedural difficulties arising from determination of jurisdiction over a networked environment.

Forum on Public Policy

Axelrod and Jay (1999, p. 14) give an example of suitable application to computer crime of an existing law. If a stolen password is used to gain unauthorized, local entry into a computer, this can be prosecuted as unauthorized use of a computer under New York State Computer Law [NYSCL], §156.05 (1998). A different example described by Axelrod and Jay (1999, p. 14) is that of a distributed denial of service attack. A distributed denial of service attack [DDoS] occurs when a multitude of networked systems direct a massive quantity of network traffic (in the form of “packets”) toward a single victim system. The deluge of packets can cause access to the victimized system to become unavailable to legitimate users. The use of computer trespass (NYSCL, §156.10, 1998) would be realistically impossible to support in court, due to the untraceable nature of a DDoS attack. Computer tampering (NYSCL, §156.20, 1998) would also be unlikely to help establish a case because, technically speaking, the intruder has not intentionally altered or destroyed computer data belonging to another person.

When Axelrod and Jay’s (1999) examples are examined, it can be seen that the “fit” between traditional law and applicability to the various network-related crimes are distinguished by the characteristic of remote connection; that is to say, the networked environment in which the crime takes place. As illustrated by Axelrod and Jay, unauthorized local physical access to a computer bears enough resemblance to the traditional laws governing trespass to allow prosecution. When certain characteristics inherently exclusive to the networked environment are introduced as in the case of a DDoS attack, laws crafted for a traditional, physical environment may prove to be difficult to apply when prosecuting the perpetrators even should the perpetrators be identified.

Traditional law in the United States has yet to precisely define jurisdiction involving cybercrime. There is little precedent concerning determination of jurisdiction over actions which

are performed remotely using the Internet as the medium for conveyance. In those cases where the United States justice system has adjudicated, “long-arm” statutes, which allow a state to extend jurisdiction to individuals or organizations not residing in that state, and local jurisdictional principals have been applied toward making decisions. Due to the paucity of jurisdiction cases involving cybercrime, there is currently a limited amount of law for policy makers or enforcement officers to reference.

Berman (2004, p. 1821) argues that “territorially-based conceptions of legal jurisdiction may no longer be adequate” in pursuing offences committed in the virtual, global environment of the Internet and proposes a pluralistic concept of jurisdiction. Berman notes a selection of cybercrime cases in which United States judges have ruled according to United States law, assuming that because United States law may apply that it should apply.

Berman’s (2004) pluralist view detaches the jurisdiction process from territorial nation-states and places jurisdiction into the virtual state occupied by networked entities represented through the Internet. Incorporating this type of view into traditional process of law would appear to be a step toward aligning viable legal strategy with the global characteristics of most cybercrime.

However, despite addressing issues of global jurisdiction, the effect of a pluralist approach to jurisdiction remains primarily reactive and only provides retaliatory action after a cybercrime has occurred. The weakness exposed in legal procedure by the lack of tangible, physical evidence exhibited by certain networked varieties of cybercrime still exists. Evidence of certain cybercrimes requires the constant audit of network activity by entities connected to the network. These types of secured entities are typically equipped with intrusion detection systems specifically designed to document and analyze network activity pertaining to dynamic states of

Forum on Public Policy

packet flow. All detection and documentation systems of this type are utilized on a voluntary basis, with little cohesive coverage of either private or public entities connected to the Internet, making recovery of digital evidence inconsistent at best. Typically, only if the organization must come into compliance with regulation, such as Sarbanes-Oxley, is this type of applied prevention consistently deployed. Where collection of tangible physical evidence is problematic, reactive strategy using traditional methods may not prove to be particularly effective at deterring those responsible for criminal activities in the networked environment.

When considering certain types of networked criminal activity, evidence gathering may simply not be feasible or possible. In these cases, preventative actions taken to secure the organization's network before the criminal activity occurs may be the only effective recourse strategy, regardless of existing cyberlaws. Applying definitions of networked criminal activity based solely on traditional reactive scenarios may be inadequate for determining which of the available reactive or preventative courses of action are more appropriate.

These issues confronting commercial, legal, and governing organizations are technically complex and increasingly expensive, in terms of lost profit, damage to reputation, and the consequences of inappropriately applied lines of defense. Conversely, cybercriminals are rapidly finding new ways to increase profit by leveraging elements unique to the online environment. An example of this new model of cybercrime is the Storm Worm, which is a worm specifically designed to generate profit for spammers. Joshua Corman, of IBM Internet Security Systems, notes "that in the past it had been assumed that web security attacks were essentially ego driven, but now attackers fall into three camps. 'I call them my three Ps, profit, politics and prestige,'" (Akass, 2007).

The problem presents itself in these stages:

Forum on Public Policy

1. Use of the Internet as a global communications tool for international commerce is becoming ubiquitous; therefore criminal activity conducted using networks and the Internet is also becoming ubiquitous as the potential for illegal profit increases.
2. Despite the availability of technical expertise, most entities lack sufficient understanding of the networked environment to enable them to make informed decisions about appropriate recourse strategies.
3. Current recourse strategies tend to depend on patchwork application of vendor-specific solutions rather than a holistic model of recourse strategies.
4. Developing a coherent taxonomy for cybercrimes is recommended to uniformly and objectively define various criminal activities. These uniform definitions allow disparate entities to more easily share information and agree on objective courses of action.

Due in part to the difficulty of extending common definitions across legal and national boundaries, and also due to the increasing automation of attack and exploit incidents, there is a growing call to selectively break with the traditional litigative reaction to cybercrime. The weight of precedent and the bureaucratic inability to deal with rapidly changing technology tends to render most organizations unable to respond adequately to this challenge. International entities tasked with governing responsibilities, as well as commercial organizations which tend to serve as the primary targets of cybercrime, appear to be generally inconsistent in applying appropriate recourse strategies.

Blitstein (2007) reports that traditional investigation and litigation is becoming increasingly ineffective: “The challenge of fighting cybercrime goes beyond resources; even some of the best detectives find it difficult adapting to the complex virtual world, where

criminals are bouncing their Internet traffic from computer to computer across several continents, and digitally laundering money through several people's bank accounts.”

The strategy model presented here, based on a technically founded taxonomy of cybercrime, is intended to aid in addressing this challenge. The model is philosophically neutral to the type and definition of cybercrime and the ontology of the model depends entirely on the technical constraints of attack attributes provided by the taxonomy. This type of neutrality addresses the need for universally accepted delineations of network perpetrated criminal behavior.

The rationale behind the model concerns the consequences of poorly chosen recourse strategies caused by misunderstanding of various criminal activities perpetrated within a networked environment. Bono, Rubin, Stubblefield and Green (2006) refer to this issue as “security through legality.” The related concept of “security through obscurity” has been well known in the field of network security for a considerable time. Over a decade ago Forrest, Somayaji and Ackley (1997) mentioned that “security through obscurity” was widely viewed throughout the network security community as a weak means of protecting systems from criminal incursion or misuse.

The concept presented by Bono et al. (2006) of security through legality exposes a similar flaw in logic. Working as network security consultants in the private sector, the researchers discovered that many system designers were delivering insecure products on the assumption that potential attackers would be deterred by the illegality of their actions.

Despite reports in the popular media concerning isolated arrests of cybercriminals, the threat of legal action does not present a significant deterrent to many types of attacker. The literature states that effective recourse is dependent on certainty of sanction (Kankanhalli, Teo,

Tan & Wei, 2003). Certainty of sanction is significantly higher in connection with system assisted exploits than in connection with system dependent exploits (Furnell, 2001), due to the resemblance of system assisted exploits to traditional criminal activity as opposed to the more automated, anonymous nature of system dependent exploits. Klepper and Nagin (1989) also found that the deterrent effect of sanctions was more directly related to the probability of detection than to the severity of the punishment associated with a given criminal activity. This would seem to indicate that passing more cyberlaws, regardless of the severity of punishment attached to a transgression, may be relatively ineffective given that certain types of cybercrime carry virtually no risk of detection. Indiscriminately classifying all types of intrusion or exploit as being equally amenable to reactive legal recourse exacerbates the growing impact of network perpetrated criminal activity upon the enterprise.

Bono et al. (2006, p. 41) recommend that the threat model for any system be founded on anticipation of “every possible thing an attacker could do,” not simply on what the attacker probably would do. This recommendation presents a broad, complex array of potential attack vectors that must be addressed in order to provide adequate security for the typical organizational networking environment. The rationale behind the strategy model presented is to attempt to order a practical approach to this array. By distinguishing criminal activity which is entirely dependent on a networked environment for perpetration from criminal activity which may merely use the networked environment as a conduit, the appropriate action for prevention or litigation may be derived.

Lough’s (2001) VERDICT criteria of taxonomy is used as the foundation for the recourse model’s taxonomy. This method uses a strategy of classification based on the common denominators revealed by Lough’s exhaustive search of the literature. These common

denominators consist of validation, exposure, randomness, and deallocation, resulting in the acronym VERDICT. All four common denominators represent a type of improper condition existing within the networked environment.

The nature of network security vulnerabilities is such that individual vulnerabilities are frequently made possible by a group of flaws. Each characteristic describes an aspect of the vulnerability being defined. In this model, a vulnerability can then be said to be the result of one or more of the characteristics defined by validation, exposure, randomness, and deallocation. The ability to apply the VERDICT taxonomy to all aspects of computer security extends the model's ability to generalize and apply definitions derived from the resulting taxonomy beyond the boundaries of specific operating systems or networking environments.

Lough (2001) specifies in the methodological description of each attribute that all attributes within VERDICT may occupy two levels of abstraction. The higher level is considered to also be the broadest, allowing the VERDICT criteria to be used for examining a system as a whole. However, for the purpose of distinguishing system dependent criminal activity from system assisted criminal activity, the lower level which depends entirely on code, protocols, and other OSI specifications was used. The higher level may, in certain cases, include social aspects which serve to blur the distinction between system dependent criminal activity and system assisted criminal activity.

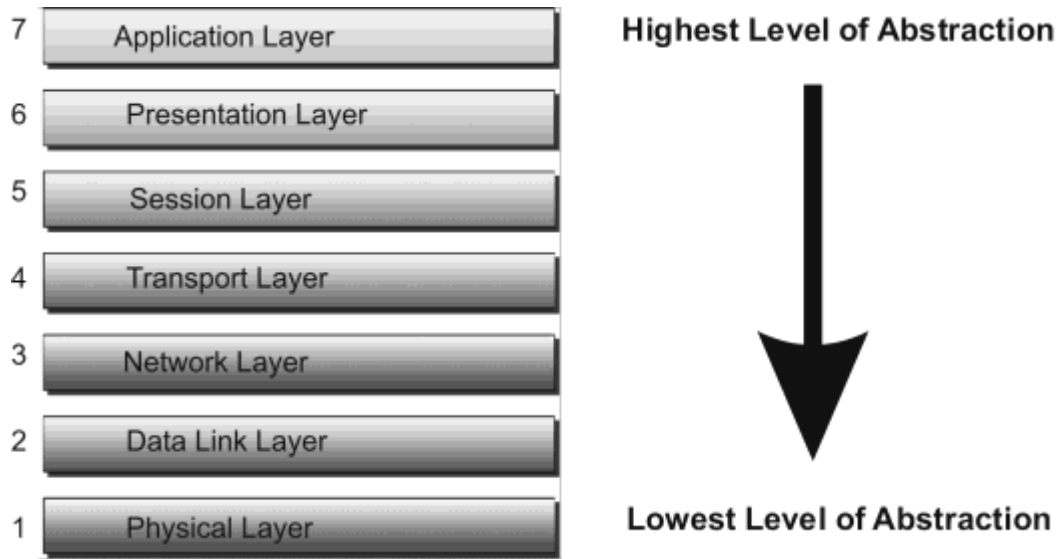


Fig. 1 : OSI model as basis for abstraction level determination

Each layer of the OSI [Open Systems Interconnection Reference] model gives detailed information concerning the networking hardware, software and protocols at increasingly primitive levels of abstraction. OSI designates the application, presentation, and session stages of the stack as the upper layers. Generally speaking, software in these layers performs application-specific functions such as data formatting, encryption, and connection management. Examples of upper layer technologies in the OSI model are HTTP, SSL and NFS. The remaining lower layers of the OSI model provide more primitive network-specific functions such as routing, addressing, and flow control. Examples of lower layer technologies in the OSI model are TCP, IP, and Ethernet.

The level of abstraction which attack attributes occupy is the key to determining the relative system dependency of the attack. Attack attributes residing at the lowest levels of abstraction, within the physical, data link or network layer, may be considered to be system dependent. These attributes define attacks that are completely dependent on vulnerabilities or characteristics of the network infrastructure, protocol or hardware. System dependent attributes

include the ability to inject or attach to existing code, the ability to propagate without a host program or user intervention, and the ability to present code to the system as a legitimate process or application. An example of an attack comprised of entirely system dependent attributes would be a distributed denial of service attack [DDoS]. A DDoS cannot be perpetrated outside of the network infrastructure.

Some attacks contain a hybridized mixture of attributes that reside at both upper and lower levels of abstraction. Viruses in particular are system dependent insofar as the malignant code is concerned, but require user intervention (an upper level attribute) in order to spread. In this regard, as a viable attack, the spread of viruses may be considered a hybrid of both system dependent and system assisted attributes.

The third category of attack attributes is system assisted. This category consists entirely of attributes residing in the higher levels of abstraction, particularly in the application level. System assisted attacks are in no way dependent on the network infrastructure, merely using the network as a means for distribution. The Nigerian 419 advance fee fraud is a system assisted attack. Previous to the widespread use of email, this criminal activity was distributed by fax, postal service and by phone, being dependent only on the gullibility of the intended victim.

After an attribute has been dissected to determine which level of abstraction it occupies, the attribute can then be appropriately classified into either the system dependent or system assisted category and placed into the taxonomy. The prototype for an automated model of the recourse strategy model uses a C4.5 decision tree to determine the relative system dependency of an attack (Quinlin, 1993). System dependency is based on the summation of an attack's attributes. By using the Boolean operations implemented by the decision tree analysis to

determine the relative system dependency of the combined attributes of an attack, the attack's most effective recourse is determined.

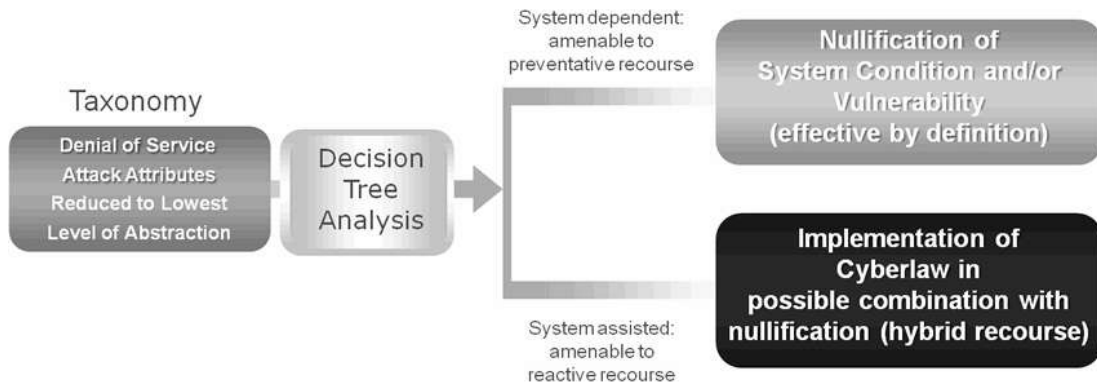


Fig. 2 : Recourse strategy model example

The significance inherent in the derivation of system dependent or system assisted attributes is the implication that defining a system-network-related criminal activity by its attributes will also define the recourse strategy most usefully deployed against the activity. If an activity can be defined as completely system dependent, it follows that the recourse strategy must also be system dependent to have an effect. The complex nature of activities defined by either completely system assisted attributes or a combination of both system dependent and system assisted attributes will require an equally complex recourse strategy. Of further significance is the understanding that recourse strategies based on system assisted attributes will have little to no effect on activities defined by system dependent attributes.

An example of this misalignment in strategy would be the passage of a cyberlaw against perpetration of distributed denial of service attacks. Because distributed denial of service attacks are entirely defined by system dependent attributes, the application of a traditional, litigative recourse strategy founded on system assisted attributes will have little to no effect on DDoS occurrence. Given that current law enforcement is under-equipped to deal with the rapidly

increasing level of cybercrime, eliminating those criminal activities which are entirely system dependent, or eliminating the system dependent attributes of a hybrid attack, by using the appropriate system dependent recourse strategy could alleviate case load while protecting networked entities.

Conclusion

As Rosu (2008) notes, the incursion of organized crime syndicates and government supported hackers into the virtual world of the Internet has supplanted the old stereotype of disaffected or curious loners hacking for the fun of it. There are now enormous profits to be made in cybercrime activities; Blitstein (2007) reports that in 2006 the FBI projected an annual loss to businesses in the U.S. alone in excess of 67.2 billion dollars. Actual losses may be higher due to reluctance on the part of many businesses to report having been hacked. The 12th Annual Computer Crime and Security Survey (2007) estimates that approximately 20% of businesses report cybercrime incidents to authorities while the majority of businesses prefer to pursue their own avenues of recourse. These figures also do not take into account the damage and expense incurred to individuals who have lost valuable data due to worms or viruses, or who have become victims of identity theft.

Liu, Yu and Mylopoulos (2003) point out that “security issues for software systems ultimately concern relationships between social actors – stakeholders, system users, potential attackers – and the software acting on their behalf” (p. 151). The majority of organizational managers are not expected to possess the depth of technical expertise required to understand the underlying differences between various computer – network – related exploits. Even so, these stakeholders are typically the individuals ultimately responsible for making network security

decisions and allocating funds to support those decisions. The average managerial stakeholder will have difficulty discerning between system assisted and system dependent exploits (Irvine & Levin, 2000) due to a lack of technical expertise and thus will have difficulty selecting effective strategies. In practice, this frequently means organizational dependence on a patchwork security solution that is likely to be understood as poorly as the technical nature of the attacks.

The proposal of the development of a model of recourse strategies presents a straightforward means by which the non-technical manager could select the most effective approach for protecting the enterprise without prior understanding of the underlying technology. This goal could be further enhanced if the recourse model served as the foundation for an automated set of strategies, implemented by decision-making software. The model's foundation on attributes categorized by dependency on the basic protocols which comprise the network infrastructure and low-level code or primitive instructions allows the user to discern any system-network-related exploit as system dependent or system assisted. Once the exploit has been appropriately defined, the most effective recourse strategy may be selected either by negating the attributes of the exploit or by seeking a litigative approach.

It is evident from the literature that law enforcement entities at this point in time do not possess the resources or technical expertise necessary to provide litigative recourse on a par with traditional criminal investigation. Until such time that law enforcement procedures in cyberspace develop a similar effectiveness to usage in a traditional physical environment, the onus of recourse must fall on the individual or organization.

Although organizations are becoming more diligent in applying network security practices due to pressure exerted by industry regulations, individuals continue to make poor network security decisions. Individuals in general agree that network security is desirable.

However, when confronted with a choice between rapid completion of a primary task and a security decision, the user is generally more motivated to complete the task and thus more likely to make an insecure decision, such as foregoing the virus scanning of a file before opening it (West, 2008).

Pursuing the universal application of a holistic model of recourse strategies, in particular a model that is objectively determined by technical specifications and standards, would yield a number of desirable outcomes. Particularly if automated by software, such a model would reduce the number of system dependent cybercrimes. It would remove part of the burden of security design decisions from the role of the non-technical manager. Some of the consequences of poor security decisions on the part of the user would be eliminated. West (2008) calls for the implementation of this type of model, saying “We must design systems with an understanding that, at some point, must make a decision regarding security.” The model of system dependent – system assisted recourse strategies proposed here is a step in that direction.

References

- New York State Computer Law*. 156. 1998.
- Akass, Clive. 2007. *Storm worm making millions a day* [Web page]. Personal Computing World 2007 [cited February 2008]. Available from <http://www.pcw.co.uk/personal-computer-world/news/2209293/storm-worm-making-millions-day>.
- Axelrod, H., Jay, Daniel. 1999. Crime and punishment in cyberspace: dealing with law enforcement and the courts. Paper read at 27th annual ACM SIGUCCS conference on user services, at Denver, CO.
- Berman, Paul Schiff. 2004. Choice of law and jurisdiction on the Internet. Paper read at Symposium on "Current Debates in the Conflict of Laws", November 12, at University of Pennsylvania Law School.
- Blitstein, Ryan. 2007. U.S. targets terrorists as online thieves run amok. *The Mercury News*, 11/13/2007.
- Bono, S., Rubin, A., Stubblefield, A., Green, M. 2006. Security through legality. *Communications of the ACM* 49 (6):41 - 43.
- Forrest, S., Somayaji, A., Ackley, D. H. 1997. Building diverse computer systems. Paper read at IEEE 6th Workshop on Hot Topics in Operating Systems.

Forum on Public Policy

- Furnell, S. M. (2001). *The problem of categorising cybercrime and cybercriminals*. Paper presented at the 2nd Australian Information Warfare and Security Conference 2001, Sydney, Australia.
- Irvine, C. E., Levin, T.E. (2000). *Toward quality of security service in a resource management system benefit function*. Paper presented at the 9th Heterogeneous Computing Workshop 2000 Proceedings, Cancun, Mexico.
- Kankanhalli, A., Teo, H., Tan, B. C. Y., Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139 - 154.
- Klepper, S., Nagin, D. 1989. The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited. *Criminology* 27 (4):15.
- Liu, L., Yu, E., Mylopoulos, J. (2003). *Security and privacy requirements analysis within a social setting*. Monterey Bay, CA: IEEE International Requirement Engineering Conference.
- Lough, Daniel Lowry. 2001. A taxonomy of computer attacks with applications to wireless networks, Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA.
- Richardson, Robert. 2007. The 12th Annual Computer Crime and Security Survey: Computer Security Institute.
- Rosu, Gabriela. 2008. Organized crime and cyberspace: a look at the evolution of organized crime in cyberspace. In *The Oxford Round Table, The Regulation of Cyberspace: Balancing the Interests*. Oxford UK: The Forum on Public Policy.
- The American Heritage® Dictionary of the English Language*. 2006. (4th) [Web page]. Houghton Mifflin Company 2000 [cited February 20 2006]. Available from <http://dictionary.reference.com/search?q=computer+crime>.
- Quinlan, J. R. (1993). *C4.5: Programs for machine learning* (First ed.). San Mateo, CA: Morgan Kaufmann Publishers, Inc.
- West, Ryan. 2008. The psychology of security. *Communications of the ACM* 51 (4):7.

Published by the Forum on Public Policy

Copyright © The Forum on Public Policy. All Rights Reserved. 2008.