Risky Business: Social Trust and Community in the Practice of Cybersecurity for Internet Infrastructure

Ashwin J. Mathew
School of Information, UC Berkeley
ashwin@ischool.berkeley.edu

Coye Cheshire
School of Information, UC Berkeley
coye@ischool.berkeley.edu

Abstract

The security of computer networks and systems on the Internet is a growing and ongoing set of concerns for nation states, corporations, and individuals. Although substantial and valuable work is in progress to secure the hardware and software technologies of the Internet, less attention has been paid to the everyday practices of the people involved in maintaining this infrastructure. In this paper, we focus on issues in cybersecurity as they apply to computer networks, to show how effective practices of network security are premised upon social relationships of trust formed within communities of cybersecurity professionals, and enacted in the practice of cybersecurity. We describe three key cybersecurity problems that involve Internet infrastructural technologies: IP address hijacking, email spam, and DNS spoofing. Through our analysis of these three problems, we argue that social trust between people – not just assurances built into the underlying technologies – must be emphasized as a central aspect of securing Internet infrastructure.

1. Introduction

The Internet is characterized by relationships of *interdependence*. Thousands of individual computer networks interconnect to form the Internet, relying on each other to carry data traffic from origin to destination. The resolution of domain names to Internet protocol (IP) addresses takes place through relations within the quasi-hierarchical structure of the Domain Name System (DNS). The delivery of some of the most common and essential data, such as email, takes place through arbitrary relations between email servers around the world.

The intertwined technological systems of the Internet are constructed through relationships between independent, autonomous organizations of people who, often invisibly, administer these interconnected systems. Thus, the practice of cybersecurity, broadly construed, is concerned with ensuring the stable, reliable operation of interdependent relationships among these human organizations as well as the technological systems they manage.

We draw on critical studies of infrastructure, to frame cybersecurity for Internet infrastructure as a system of inter-related social and technological elements [26][27][28]. Studies of infrastructure have, in general, focused on the processes through which infrastructure is designed, developed and deployed, at scales ranging from localized project-specific contexts to a societal level. In contrast, we are concerned with infrastructural mechanisms of relative stasis, rather than change: once deployed, how is an infrastructure maintained as a stable, ordered system? This is not to say that infrastructure is static in our view, but that relative stasis – predictable, repeatable behavior – is a primary goal for infrastructure once deployed, just as much as relative change (however slow) is a primary goal for infrastructure in the process of design, development and deployment. A focus on relative stasis in infrastructure calls to attention the processes through which failures occur and are managed to assure order and stability in infrastructure. The analysis of the relationship between relative stasis and failure requires study of problems of risk in infrastructure, and the associated practices and structures involved in maintenance (as responses to unintentional, but possibly anticipated, failures) and security (as responses to intentional attacks).

The issues of maintenance and security for infrastructure become substantially more complex once we consider problems of interdependence: the stable operation of an infrastructure is premised upon stable relationships between interdependent systems, as much as on the stable operation of the individual systems themselves. This is especially true when the socio-technical relationships between the interdependent

URI: http://hdl.handle.net/10125/41438
ISBN: 978-0-9981331-0-2

systems composing an infrastructure cut across territorial and organizational boundaries, as is the case with the Internet in general, and cybersecurity in particular.

A key problem that any relationship of mutual interdependence must address is what is at stake in an interaction, which is most commonly referred to as *risk* [5]. To date, the dominant view on cybersecurity is that risk can be managed through primarily technological solutions, assisted by economic analysis of incentives and appropriate legal frameworks [20][21][22][23]. As we argue, however, such solutions invariably underestimate the critical importance of the social relationships within the communities of technical personnel who manage and control these infrastructural technologies. In our view, trust as a social solution to managing risk has received insufficient attention in the analysis and design of the Internet's infrastructural technologies, especially from a perspective of cybersecurity. We argue that social trust is inherent to the interdependent nature of the Internet infrastructure, and it must be considered as a central problem in cybersecurity.

In this paper, we detail the specific ways in which risk manifests – and is managed – in three distinct infrastructural technologies of the Internet. To evaluate these cases, we draw from three years of ethnographic fieldwork in communities of the Internet's technical personnel, across North America and South Asia, spanning regional professional organizations and global governance bodies, which we detail below. Our aim is not to provide a comprehensive empirical analysis of each of the cases from this larger research, but rather to summarize and contextualize these cases as significant illustrations in support of our argument.

First, we examine the problem of IP address hijacking, a class of attack in which one computer network claims to host a range of IP addresses which in actuality are hosted by another network. Second, we present the problem of email spam, which is among the most easily visible forms of risk that Internet users commonly experience. Finally, we analyze the problem of DNS spoofing, in which a DNS server sends spurious responses to clients, directing them to IP addresses other than those of the service which they requested.

We chose these three cases because they each illustrate different types of risk that must be mitigated in order to maintain the security and reliability of the Internet infrastructure. Through a descriptive analysis of these three problem areas, we show how *social trust* is integral to the practice of operating the technological infrastructure of the Internet. We focus on the nature of interdependence in the technological system, the quality of the risks that result, and the role that social trust relations play in the management of these risks. Finally, we conclude our analysis with a series of specific recommendations about how social trust can be emphasized in both the study and practice of maintaining a secure and reliable Internet.

2. Trust and Interdependence

Trust is a complex construct that has many different definitions and meanings in social science, computer science, and related disciplines. However, all conceptions of trust seek to address a common problem: the management of expectations in the face of potentially risky, uncertain interactions. Before applying the concept of trust to our specific cybersecurity problems, we first review the key differences in trust and trust-related terms.

Individual models of interpersonal trust focus on why one person might choose to take a risk on another, calling attention to individual attitudes, emotional content and cognitive dimensions. Since no-one can ever have complete knowledge to anticipate another person's behavior, the ability to trust is essential to social interactions [1]. In contrast, system trust describes the trust that individuals must have in the infrastructures – such as water, electricity and communications – that support everyday life. In the absence of any meaningful understanding or power over how these infrastructures function, the trust that individuals have in the reliable operation of these infrastructures is premised upon confidence that they will not fail, rather than an active choice taken with knowledge of risk [2][3].

Since our concern is with interdependence in social-technical systems, we adopt a model of trust which takes human relationships as its primary building block [4][5][6]. In this model, trust is conceived of as a three part relation, in which one person trusts another in relation to a specific action. For instance, it is not uncommon for individuals to ask strangers to watch their bags at the airport for a few minutes, but it is unlikely that someone might ask a stranger to watch a child in the same context. Trust is not merely a matter of the relationship between two

people, but also of the magnitude of the risks in a particular context.

In the above examples, an expectation of trust is made possible through the evaluation of whether or not a person is trustworthy. At an airport, this might simply be a matter of trust-warranting cues [6]: for example, what the stranger looks like, how they are dressed, etc. In ongoing interactions, however, the evaluation of trustworthiness may arise from reputation constructed through knowledge of prior interactions. For instance, a regular customer of a neighborhood shop may be trusted by the shop owner to run up a tab, while a customer visiting the shop for the first time would likely be asked to pay immediately.

This conception of trust implies an ability to choose whether or not to trust, and whom to trust: in the absence of choice, what is colloquially referred to as 'trust' may be better described as a confidence in expected outcomes [7]. Confidence is made possible through assurance structures which are designed to minimize risk. Assurance structures may be centralized authorities (as in central banks assuring that paper money has value) or social norms (as in punishments such as exclusion or other penalties) which ensure that expectations are met in social relationships [8]. In everyday life, ongoing interpersonal relationships between parties often function through some mix of trust and assurances.

Trust relationships and assurance structures are produced and reproduced in professional communities and institutional forms, and enacted in the everyday practice of administering Internet infrastructure. Individuals enter into trust relationships in order to be effective in their practice, forming these relationships through engagement with communities of practice [9] of technical personnel involved in managing the everyday operation of Internet infrastructure. These communities, practices and trust relationships are in turn anchored by assurance structures, which encompass behavioral norms in the operation of technology (often characterized and documented as "best practices") as well as organizational forms specialized to administer particular aspects of technology.

We follow these lines of analysis in the cases we present below, to show that while the nature of risk and uncertainty can and should be characterized in technological terms, the responses to risk and uncertainty must be analyzed in terms of practices engaged in by professional communities, enabled through social trust relationships and assurance structures.

3. Methods and Materials

The cases we present in the sections which follow are based on three years of ethnographic fieldwork in communities of the Internet's technical personnel across North America and South Asia. Over 50 semi-structured interviews were conducted in the course of this research, alongside participant observation during meetings and conferences of professional associations and governance bodies involved in the operation of Internet infrastructure. In addition, a variety of textual materials generated by the technical communities represented by these organizations were analyzed, including email lists, best practices documents, policy documents and standards documents.

Fieldwork was concentrated on regionally organized professional communities of network administrators in North America and South Asia: the North American Network Operators Group (NANOG) and the South Asia Network Operators Group (SANOG). In addition, fieldwork was conducted at the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), a consortium broadly representative of the email industry, the Internet Engineering Task Force (IETF), which sets technical standards for Internet infrastructure, and the Internet Corporation for Assigned Names and Numbers (ICANN) which oversees the unique allocation of resources (such as domain names and IP addresses) for the global Internet.

We chose these particular professional communities since they presented a basis for the analysis of interrelationships in Internet infrastructure across geographies and functions. The relational comparison between NANOG and SANOG serves to illustrate the differences and connections between the North American context, which is relatively central to Internet infrastructure, and the South Asian context, which is relatively peripheral. Research into the M3AAWG, IETF and ICANN alongside NANOG and SANOG supported the analysis of the relationships between the everyday practices of network operations, and the functions of industry coordination, standards development and resource allocation for Internet infrastructure. For a detailed discussion and analysis of the themes from this research, see [24].

4. Risk in Interdependent Systems: Three Cases

In the cases which we present here, we build on the concepts established in the prior section. In each case, we describe the nature of risk and interdependence in the technological system under study. We then examine the combination of trust relationships and assurance structures – and the professional communities, practices and organizational forms through which these are realized – that stabilize and order the technological system. As we will show, social trust is an integral component of the practice of managing these systems, and must be understood as such, rather than as a problem to be engineered away.

4.1. IP Address Hijacking

As of this writing, the Internet is composed of over 55,000 interconnected computer networks [10]. Each computer network originates one or more blocks of IP address space, which are used to address computers located within that network. IP address hijacking occurs when one network attempts to capture data traffic actually intended for another network.

Networks can carry traffic intended for other networks, and in fact often need to do so. A network operated by an organization, or an Internet service provider, may pay a larger network which provides regional connectivity, to carry data traffic within a geographical region. A regional network may in turn pay an even larger network to carry traffic across regions, and continents. It is through this system of interconnections between networks, spanning different geographical scales, that the global Internet is realized.

The technology which enables the interconnection of networks is called the Border Gateway Protocol (BGP). Using BGP, networks announce the IP address blocks to which they can carry traffic to their neighboring networks. These neighbors in turn announce these IP address blocks to their neighboring networks, and so on. If the same IP address block is received from two neighbors (i.e., there are multiple possible routes to the same destination), a network administrator configures local routing policy to prefer one neighbor over another, depending on a range of variables, such as bandwidth and diversity of points of interconnection and the cost of carrying traffic. The result is a distributed routing system – called the inter-domain routing system – through which every network has knowledge of which neighbor it should use to reach a particular IP address.

BGP is amongst the most essential infrastructural technologies of the Internet. In the absence of the interconnections enabled by BGP, there would be no Internet.

As critical as BGP is to the correct functioning of the Internet, it provides no mechanisms for a network to establish the veracity of the routing claims received from neighboring networks. Any network may claim to be able to carry traffic to any IP address block using BGP. Immediate neighbors can verify the authenticity of these claims for IP address blocks which a network is authorized to originate (i.e., for IP addresses which reach computers within that network). However, it is much more difficult to establish veracity when dealing with routing announcements claiming the ability to carry traffic to IP address blocks in remote networks. In order to reach a given destination IP address, traffic from one network often needs to transit several intermediary networks. The network from which the traffic originates has no way of knowing whether or not any of these intermediaries can actually carry the traffic to its intended destination.

Although the everyday experience of the Internet is stable – traffic is correctly delivered to expected destinations – spurious announcements of routing information in BGP are not an uncommon occurrence, whether as mistakes of configuration, or as intentional efforts to redirect and capture traffic [11][12][13]. These kinds of attacks are known as IP address hijacking, in which one network hijacks traffic intended for the IP address blocks of another network.

The only effective remedy currently in place against IP address hijacking is the “prefix filter”, which is documented as a best current practice by the Internet Engineering Task Force (IETF), which sets technical standards for the Internet [14]. If a network knows the list of IP address blocks which a neighbor is authorized to originate, it may use a prefix filter to block the announcement of any IP address blocks outside the authorized list. This approach works well when a network is dealing with neighboring networks who only announce their own IP address space (such as a campus network, or a data center), and do not carry traffic for any other networks.

However – as we have already noted – it becomes infeasible to apply prefix filters when dealing with networks which do carry traffic for other networks.

Under these conditions, the only meaningful response is one of trust. Administrators responsible for operating a network must trust that their counterparts in neighboring networks will follow best practices in securing their networks, and ensure that they will not be the source of an IP address hijacking event. In the process of setting up and maintaining an interconnection between networks, administrators in each network will often have to communicate with each other, and in the process form a sense of each other's competency, and over repeated interactions build a social relationship of trust. In the instance that a prefix hijacking event (or other network security issue which affects neighbors) occurs, both the technical relationship of interconnection and the social relationship of trust will be re-evaluated, and in extreme cases, terminated. Commenting on the importance of interpersonal trust relationships, a network administrator told us, "[trust] is pretty big because if you've got a good contact in your upstream [network] for example, and you can at least talk to them, and get something done, or if there's nastiness emanating from one particular network, then it's good if you can talk to somebody because really, if you don't have good contacts, the chances of influencing anything is pretty slim really, right."

It is not only in the practice and process of network interconnection that social trust relationships are formed between network administrators. Trust relationships are also formed at meetings of regionally organized professional communities of network administrators, such as the North America Network Operators Group (NANOG), the South Asian Network Operators Group (SANOG), and many more. Meetings of these groups typically occur between 2 and 3 times every year across locations within their geographies, with ongoing discussion of computer networking issues on dedicated email lists. Socializing in person, making presentations, and participating in workshops at these meetings all contribute to the formation of social trust relationships between attendees, and the evaluation of reputation (for running a well-behaved network, and for technical knowledge) within a community. A senior member of the NANOG community summed up these dynamics in an interview: "Certainly NANOG is one of the places … where you can become a trusted individual … where you can get up and talk about problems that you're seeing in the network, to get other people together that are seeing the same problem, to generate more push to get the processes changed, and [Internet Service Providers] work with each other. I see that as very important."

The stability of the critical Internet infrastructure of interconnections between networks is assured through trust relationships formed in the practice of network interconnection and in professional communities of network administrators.

4.2. Email Spam

Email spam is a problem that is almost as old as the Internet itself [15]. Whether as advertising, scams, or other communications, email spam is universally unwanted.

The fundamental problem for email is one of openness, which is similar in many ways to that for network interconnection. Just as network interconnection should allow any IP address on the Internet to send and receive any traffic from any other IP address, email assumes that any email server should be able to send and receive any email from any other email server. Open systems provide for great autonomy and ease of interconnectivity, but introduce significant problems of interdependence at the same time. Anyone can set up an email server under their own control, configure it as they wish, and immediately be able to send and receive email from any other email server with no additional effort. The problem, of course, is that such an open system also provides the grounds upon which spam may be sent and received with similar ease.

A common defense against spam, which anyone who uses email is familiar with, is the spam filter, which attempts to distinguish spam from legitimate email. However, spam filters only sort spam at its destination, once it has been delivered. From a network security perspective, it is preferable to stop spam as close to its origin as possible, to save bandwidth, storage and processor cycles for email servers. This is especially concerning, since recent estimates indicate that spam is well over 50% of all email [16]. In this section, we describe the mechanisms through which network level anti-spam efforts are made possible.

In the early days of the Internet, stopping spam was often simply a matter of contacting the administrator of the email server originating spam, and asking them to suspend the offending email account. This was a viable approach at the time, since there was a relatively small number of email servers, and most email server

administrators knew one another [15]. As the Internet grew, and the number of email servers increased, it became unreasonable to combat spam through personal relationships among email server administrators. In contrast with BGP, where each computer network is directly connected to only a limited set of other computer networks, every email server is potentially connected to every other email server on the Internet, drastically increasing the complexity of interdependence in this system.

The solutions to the problem of spam have therefore necessarily taken the form of assurance structures. A variety of for-profit and non-profit entities (such as SpamHaus, SORBS, SpamCop and others) provide regularly updated lists of email servers that are primarily sources of spam which should be blocked. Block lists vary from being manually maintained, to those which look for patterns of spam in email to automatically identify spam sources. Email server operators may choose to subscribe to one or more of these block lists to identify email servers from which they should not accept any inbound email, or which they treat as a spam source to which additional policy must be applied before delivering email.

In the instance that an email server operator feels that they have been wrongly categorized as a spam source by a block list, they must follow guidelines published on block list websites to facilitate their removal. These guidelines are typically purely technical in nature, such as requiring that the proportion of spam has been below a certain threshold for a certain period of time before removal from the block list.

The relationship between email senders, email receivers and block lists is complicated by the fact that advertisers (or email services providing support for advertisers) do need to send large quantities of email, while at the same time avoiding being listed on block lists. In many ways, the behavior of a large advertiser can resemble that of a spam source. The notion of what is, and is not, spam is no longer as straightforward when considering these commercial relationships.

The organizational space in which these tensions are worked out in practice is the Messaging, Mobile and Malware Anti-Abuse Working Group (M3WAAG). This is an international industry consortium which was initially created as a space for coordination between email services, and later expanded to include issues of messaging on mobile phones, and of malware. M3AAWG meets three times a year, across locations in Europe and North America, with ongoing communications on several email lists. Presentations and discussions at M3AAWG often deal with making sense of best practices among the diverse interests represented at M3AAWG. These discussions may eventually be published as best practice documents, for consumption beyond the core M3AAWG membership. For instance, the Vetting Best Common Practices document [17] deals with processes that email service providers should follow in signing up new customers, to ensure that these customers do not use the email service provider's infrastructure to send spam. Over lunch at a M3AAWG meeting in San Francisco, a Brazilian email operator related his interests in attending the M3AAWG meeting, in spite of the time and money involved in travel from Brazil: “this is a place to network, to build trust amongst different groups, coordinate and collaborate, and get a sense of what different parties' interests are: hosting providers, email service providers, law enforcement…”.

Attendance at M3AAWG meetings is limited to employees of M3AAWG member organizations and their guests. Admission to membership in M3AAWG is controlled by the M3AAWG board, which adjudicates new membership applications – and conducts annual reviews of existing memberships – based on whether or not an organization is recognized as a responsible well-behaved actor within the messaging ecosystem.[1] Unlike the regional network operator groups surveyed in the last section, which are open for anyone to attend, M3AAWG intentionally limits attendance to ensure that bad actors are unable to participate in the sense-making around the policy and practice of messaging. For example, our attendance at M3AAWG meetings was only made possible through a guest invitation facilitated by a M3AAWG member organization. Every presentation we attended at M3AAWG was prefaced with a notice reminding attendees that the contents of the presentation were not to be publicized outside the context of the M3AAWG meeting.

Even though the everyday practice of combating email spam relies on the assurance structures of block lists, the processes through which notions of best practice and policy are formed take place through trust relationships in a professional community anchored by the organizational form of M3AAWG.

[1] See https://www.m3aawg.org/join for details, last retrieved June 9th, 2016.

4.3. Domain Name Spoofing

The Domain Name System (DNS) provides the means through which a human-readable name for a service on the Internet is resolved to an IP address through which to reach the computer system providing the service. DNS is used in almost any interaction that occurs in everyday use of the Internet, resolving names to IP addresses for web servers, email servers, file servers, and more. Accordingly, there is great power in the operation of DNS servers: a rogue DNS server operator may spoof domain names, resolving domain names to IP addresses of their choosing, intercepting all traffic to those domain names, and modifying it at will, potentially impersonating a service to gather login credentials and other sensitive information.

DNS functions through a hierarchy of servers. Whenever a lookup is performed on DNS, the request initially goes to one of the root servers, which returns the IP address of the server for the top-level domain (such as ".com", ".org" or ".net") in the requested domain name. The request is then redirected to the server for the top-level domain, which in turn returns the address of the server for requested domain (such as "hicss.org"). This process may continue, recursively, until all dot-delimited names have been exhausted to find the IP address of the machine providing a particular service (such as "www.hicss.org").

The apparently hierarchical structure of DNS is complicated by the fact that Internet service providers and other large organizational networks (such as campus networks) may operate their own local DNS servers. Whenever a user within a network looks up a domain name, the request goes to their local DNS server, which then mediates the process of recursively resolving the domain name from the root DNS servers. Local DNS servers are points of control at which the resolution of domain names to IP addresses may be spoofed.

In response to the problem of domain name spoofing, a set of extensions to secure DNS were developed by the Internet Engineering Task Force, collectively termed DNSSEC. These extensions provide mechanisms for end user systems to detect spoofing, and alert users to such behavior. DNSSEC functions by cryptographically signing the root DNS zone, which holds all top-level domains, and is maintained on the DNS root servers. Each top-level domain server in turn cryptographically signs all names which it hosts, and so on down the hierarchy of DNS servers. Each key used for cryptographically signing a level of the DNS hierarchy is itself signed by the key of the level above. As a result, an end user system can verify a technological chain of trust leading to the root zone, and detect if this chain has been modified in any way.

The problem is that such an arrangement is premised upon a single root cryptographic key to maintain both authentication and control over the whole system. The introduction of DNSSEC led to concerns in DNS operator community over accountability in the control and use of the root key.

The root key for DNSSEC is maintained by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit entity which oversees the management of domain names, IP addresses, and other critical Internet resources for the global Internet. In the process of deploying DNSSEC, ICANN created the Trusted Community Representative position. Trusted Community Representatives are members of the Internet's technical community who observe the key signing process at data centers operated by ICANN, and hold fragments of root key, to allow it to be reconstituted in the event that it is lost.[2]

As much as the Trusted Community Representatives play an important role in maintaining the root key, they play an even more important role in securing the legitimacy of ICANN's control of DNSSEC. As several DNS operators told us, even though they might not trust ICANN as an organization, they trust ICANN's operation of DNSSEC insofar as people who they trust – appointed as Trusted Community Representatives – vouch for the integrity of the DNSSEC process. The assurance structure for DNSSEC gains legitimacy from trust relationships and reputation maintained by Trusted Community Representatives within the broader communities of administrators who are responsible for operating DNS servers, and implementing DNSSEC for their own domains.

5. Trust in Technology, Trust in People

Each of the three cases surveyed above deals with distinctively interdependent technological forms, but the solutions to risk and uncertainty in each case may be made understood in terms of social trust

[2] For a list of Trusted Community Representative, see https://www.iana.org/dnssec/tcrs, last retrieved June 9th, 2016.

relationships articulated through professional communities and practices. In each case, combinations of trust relationships and assurance structures serve to stabilize and order interdependent technological systems, balancing individual autonomy and centralized control.

IP address hijacking is mitigated through the technological mechanism of prefix filters, and social relationships of trust in the practice of interconnecting networks. These trust relationships and practices are produced and reproduced in professional communities of network administrators. The result is a system which has a high degree of autonomy for individual computer networks, and very little centralized control.

Block lists represent the key technological assurance structure through which email spam is mitigated. Email service providers and block list providers have substantial autonomy in their operations, and very little direct control over each another. Instead, coordination and collaboration occur among these diverse actors through trust relationships formed within the restricted community of M3AAWG, in the interests of constructing and evaluating trustworthiness, and collective sense-making for the practices and policies involved in operating email services.

DNSSEC provides a highly effective antidote to domain name spoofing, but at the cost of a certain degree of autonomy for DNS server operators. The legitimacy of ICANN as the assurance structure maintaining the root key for DNSSEC needs the support of Trusted Community Representatives: technologists with strong reputations and trust relationships in the broader technical communities responsible for deploying and operating DNSSEC.

Across these cases, trust is not a social value embedded in technological form so much as it is necessary element of technological practice, realized in social relations and communities. Efforts to secure computer systems and networks often focus on implementing more secure "trustworthy" technological forms. While we do support these efforts, we approach them with the caution that they provide surety, or confidence, rather than trust [18], reposing all authority in technology, often implemented through strong assurance structures of centralized control. Such systems are potentially brittle, susceptible to global technological failure, and political capture of centralized controls. In contrast, a system which privileges social trust relationships is prone to local failures, but more resilient as a whole, though it requires substantial investment in distributed communities and practices for reliable operation.

Here lies the trust paradox: highly autonomous systems with weak assurance structures lead to strong trust relationships, while highly controlled systems with strong assurance structures do away with the need for trust relationships [19]. As we have argued, the answer is not to choose either trust relationships or assurance structures, but to imagine a combination of both. A trustworthy computing system may be designed with a strong assurance structure; but this assurance structure still needs legitimacy from the communities of practice who will be subject to it in order gain acceptance for its authority. Similarly, a computing system may be designed with strong trust relationships in mind; but this system will still need to take into account the effort involved in developing professional communities of practice to anchor these trust relationships, and the potential assurance structures which may yet be required by the system.

6. A Path Forward: Accounting for Social Trust in Internet Infrastructure

Cybersecurity is typically characterized in terms of problems of attack and defense, of incentives and compliance, and of technological design. While all of these are necessary and valuable approaches to cybersecurity, we argue that the application of cybersecurity to interdependent systems – such as those which we have described here – calls for attention to problems of social trust.

It is necessary, but not sufficient, for instance, to examine incentive structures for the deployment of secure extensions to technology, such as DNSSEC. Equally, the political problem of maintaining the legitimacy – the trustworthiness – of the authority managing the DNSSEC root is a critical issue. Incentives and legal regimes can account for the forces driving competing organizations together in the formation of M3AAWG. However, these alone are insufficient to understand the functioning of M3AAWG as a community with a restricted membership forming trust relationships and common understandings of practice around the mitigation of email spam. Similarly, the function of professional communities of network operators cannot be explained only in terms of incentives and regulations around

particular aspects of network interconnection. Thick relationships of trust and common understandings of practice are formed within these communities, easing the coordination and collaboration needed in the everyday practice of network interconnection.

The design of new technologies intended to provide more secure networked computing environments must take into account the social trust required in the practice of operating these systems. This is especially true when a system is composed of interdependent components, spanning territorial and organizational contexts. In such cases, professional communities of technical personnel responsible for the everyday operation of these systems must be seeded and supported to provide spaces for the production of trust relationships and sense-making around shared concepts of "best practices" for operating these systems. For example, NANOG was created and initially funded under the auspices of the US National Science Foundation, to support a professional community for coordination between the technical personnel involved in operating the computer networks of the early Internet [24].

At the same time, careful attention must be paid to the technological form of the system. Does it require a single central authority for its reliable operation? Does it allow for multiple optional authorities? In each case, the question of how these authorities might maintain their legitimacy and trustworthiness is critical, and must be addressed with the technical communities who rely on these authorities in their everyday practice. These kinds of issues are very apparent in the deployment of DNSSEC, and in ongoing efforts to secure BGP which similarly rely on centralized authorities to assure security [25].

The functioning of the interdependent systems of Internet infrastructure must be understood in terms of shared understandings of practice, formed between geographically distributed communities, supported by trustworthy assurance structures. Such analysis is complicated by variations in market structures and legal regimes across geographies and over time, alongside evolutions in technological form. These varying pressures can be difficult to make sense of, both internally for those involved in operating a system, and externally, for those aiming to analyze existing systems and design new systems. However, social trust relationships offer the necessary lubrication and glue to ease and maintain the operation of these systems in the face of complex interactions of market structures, legal regimes and technological forms [24].

These are but a few guidelines for thinking about how to support trustworthy social operational environments for secure networked computing systems, as necessary adjuncts to technological, economic and legal analysis. Through the ongoing growth and evolution of these systems, it is important to continue to pay attention to the ethical dilemmas and social norms which emerge in the practices of technical communities. As the cases which we have presented illustrate, there are ample precedents in the development of Internet infrastructure to draw from in thinking about the design of future secure technologies.

Designing systems with social values of trust in mind is as much a political and social problem as it is a technological problem. It is essential that social trust be taken as a primary object of study in the analysis of the complex interdependent systems which make up the critical infrastructure of the Internet.

Acknowledgements

We would like to thank the anonymous reviewers who provided invaluable feedback on this paper. The research for this paper was supported by a grant from the UC Berkeley Center for Long Term Cybersecurity, and a fellowship at the Slow Science Institute.

References

[1] J. D. Lewis and A. Weigert, "Trust as a Social Reality," *Soc. Forces*, vol. 63, no. 4, 1985, pp. 967–985.

[2] N. Luhmann, *Trust and Power*. John Wiley and Sons, 1979.

[3] A. Giddens, *The Consequences of Modernity*. Stanford University Press, 1991.

[4] R. Hardin, *Trust and Trustworthiness*. Russell Sage Foundation Publications, 2002.

[5] K. S. Cook, T. Yamagishi, C. Cheshire, R. Cooper, M. Matsuda, and R. Mashima, "Trust Building via Risk Taking: A Cross-Societal Experiment," *Soc. Psychol. Q.*, vol. 68, no. 2, 2005, pp. 121–142.

[6] C. Cheshire and K. S. Cook, "The Emergence of Trust Networks: Implications for Online Interaction," *Anal. Krit.*, no. 26, 2004, pp. 220–240.

[7] N. Luhmann, “Familiarity, Confidence, Trust: Problems and Alternatives,” in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. Basil Blackwell, 1988, pp. 94–107.

[8] T. Yamagishi and M. Yamagishi, “Trust and Commitment in the United States and Japan,” *Motiv. Emot.*, vol. 18, no. 2, pp. 129–166, 1994.

[9] J. Lave and E. Wenger, *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, 1991.

[10] G. Huston, “CIDR Report.” [Online]. Available: http://www.cidr-report.org/as2.0/.

[11] P. Boothe, J. Hiebert, and R. Bush, “How Prevalent is Prefix Hijacking on the Internet?,” in *Proceedings of NANOG36*, 2006.

[12] V. Khare, Q. Ju, and B. Zhang, “Concurrent Prefix Hijacks: Occurrence and Impacts,” in *Proceedings of the 2012 ACM Conference on Internet Measurement*, 2012, pp. 29–35.

[13] A. Ramachandran and N. Feamster, “Understanding the Network-level Behavior of Spammers,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, 2006, pp. 291-302.

[14] J. Durand, I. Pepelnjak, and G. Doering, “RFC 7454/BCP194: BGP Operations and Security,” 2015. [Online]. Available: https://tools.ietf.org/html/rfc7454.

[15] F. Brunton, *Spam: A Shadow History of the Internet*. MIT Press, 2013.

[16] Darya Gudkova, M. Vergelis, N. Demidova, and T. Shcherbakova, “Spam and phishing in Q1 2016.” Kaspersky Lab, 2016.

[17] Messaging Anti-Abuse Working Group, “Vetting Best Common Practices,” 2011. [Online]. Available: https://www.m3aawg.org/sites/default/files/document/MAAWG_Vetting_BCP_2011-11.pdf.

[18] H. Nissenbaum, “Will Security Enhance Trust Online, or Supplant It?,” in *Trust and Distrust in Organizations: Dilemmas and Approaches*, K. M. Roderick and K. S. Cook, Eds. Russell Sage Foundation Publications, 2004, pp. 155–188.

[19] E. Gellner, “Trust, Cohesion, and the Social Order,” in *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta, Basil Blackwell, 1988, pp. 142–157.

[20] D. K. Mulligan and F. B. Schneider, “Doctrine for Cybersecurity,” Daedalus, vol. 140, no. 4, 2011, pp. 70–92.

[21] F. B. Schneider, Ed., Trust in Cyberspace. Washington, D.C. The National Academies Press, 1999.

[22] United States Government, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” 2009. [Online]. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[23] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Trans. Dependable Secur. Comput., vol. 1, no. 1, 2004, pp. 11–33.

[24] A. J. Mathew, “Where in the World is the Internet? Locating Political Power in Internet Infrastructure,” Ph.D dissertation, University of California, Berkeley, 2014. Available: http://www.ischool.berkeley.edu/files/ashwin-dissertation.pdf

[25] A. J. Mathew and C. Cheshire, “The New Cartographers: Trust and Social Order within the Internet Infrastructure,” in Proceedings of the 38th Research Conference on Communication, Information and Internet Policy (Telecommunications and Policy Research Conference), 2010.

[26] P. N. Edwards, “Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems,” in *Modernity and Technology*, edited by T. J. Misa, P. Brey, and A. Feenberg, MIT Press, 2003, pp. 185–226.

[27] T. P. Hughes, “The Evolution of Large Technological Systems”, in *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, edited by W. E. Bijker, T. P. Hughes, and T. J. Pinch, MIT Press, 1987, pp. 51–82.

[28] S. L. Star, “The Ethnography of Infrastructure”, American Behavioral Scientist 43, no. 3, 1999, pp. 377–91.