

Security or Privacy, Must We Choose?

(Position Paper)

Mike Burmester,* Yvo Desmedt,* Rebecca Wright,** Alec Yasinsac*

*Department of Computer Science
Florida State University
Tallahassee, FL 32306-4530

**AT&T Labs Research
180 Park Avenue
Florham Park, NJ 07932

Abstract

Hardly a day passes without reports of new threats in or about the Internet. Denial of service, worms, viruses, spam, and divulged credit card information highlight the major security threats. At the same time, we are bombarded by reports that privacy is at the greatest risk of all time, caused by the massive ability to store and search information and to trace activities across the Internet. In this paper, we address issues of conflict that exist between security mechanisms and privacy, including the tradeoffs from a public safety and well-being standpoint, and the technology that can facilitate a suitable balance between privacy and protection priorities. The recent brutal attacks at the World Trade Center and the Pentagon on Sept 11, 2001, confirm the connection between security, privacy, and public safety. To protect our liberties and freedoms it is therefore essential that we adopt a holistic security approach.

1. Introduction

Though computer and network security, and indeed computer science itself, are new fields, it was recognized rather early on that security and privacy are intimately linked. Through the years, the meaning of the term privacy has evolved. In this paper we address the issue of personal privacy, and analyze the conflict between computer and network security goals and personal privacy.

As we often see in other fields, an attempt to solve one problem may trigger another problem. In this paper we address how security and protection goals and mechanisms impact on personal privacy, and offer alternatives to existing paradigms. We begin the discussion in Section 2 by identifying computer- and network-related threats to critical infrastructures and some of the current security approaches used to protect these infrastructures. In Section 3, we discuss privacy and the role of accountability in infrastructure protection, and the apparent inherent conflict between them. In Section 4, we propose "accountable privacy", whose goal is to provide a balance between these competing priorities. We conclude in Section 5.

2 Security

2.1 Threats to the Infrastructure

We consider a broad definition of infrastructure, where any system component that provides a routine service is part of the infrastructure. A characteristic, then, is that other components that are dependent on the infrastructure may fail due to failure of an infrastructure component. From this perspective, many computers and other electronic components that carry electronic traffic are infrastructure components. Networks, as they are known, are certainly consumers of the electronic communication

service they provide, but their purpose is to provide service to end users. Clearly, when the network fails, users that are dependent on network service may fail as well.

Mechanisms that provide secure communication over insecure infrastructure have been proposed. By our definition, the cryptographic techniques these mechanisms employed are themselves infrastructure components and face the same challenges as the rest of the network.

2.2 Threats to networks

Threats to networks come in many forms and are naturally hard to categorize. From a security standpoint, a network should (at least) support confidentiality, integrity, and availability of electronic communications. That is to say, the network should: (a) employ components that ensure confidentiality to the desired level, (b) provide facilities that allow users to protect their communications from compromise, and (c) provide facilities that allow users to guarantee availability to their desired level of confidence.

2.3 Dependability

To be dependable, a network must provide the expected service, the *way* that is expected, and *when* it is expected. In particular, failure to remain dependable will result in end user systems not being available, and thus, limit the use of the network. We see some results of this in the Internet today, as e-commerce has dropped dramatically. No doubt this is due in part to the present widespread economic downturn, but possibly also a result of the many security breaches, such as loss or publication of credit card information. Clearly, without sufficient protection, e-commerce cannot thrive. Apart from e-commerce, the entire economy is largely dependent on networks: airlines depend on networks to make flight reservations; the vast majority of funds transfers are electronic; many power grids depend on network communication to control power production and distribution; and the list goes on. It is truly a challenge to find any significant aspect of daily life that is not dependent on the network resource in some critical way. For this reason, the network infrastructure must be aggressively protected.

In this paper, we do not limit ourselves to failure as a result of normal wear, component faults, or other normal operational failures, but rather focus on the more difficult problem of malicious failures resulting from intrusions, attacks, hacks, and other intentional misuse by people.

Direct security threats to network dependability include distributed denial of service attacks, viruses and worms, web page defacement, “stealing” information recorded or transmitted in the network for unauthorized use, inappropriately modifying network traffic, and masquerading. Protecting networks against such threats is a target-rich research and market field.

2.4 Security Approaches and Mechanisms

The goals of information security are to: (a) *prevent*, or (b) *detect and respond* to attacks and misuse of computer and network resources. The latter is only necessary because the former is not sufficiently achievable. Access control mechanisms bear the brunt of the protection weight of existing networks, bolstered today by a plethora of tools from virus scanners to firewalls. The majority of these approaches require an ability to determine the identity of a party to the communication, a process known as (entity) authentication. We will discuss authentication in greater detail as we address the different aspects of privacy.

The recent emphasis on packet filtering and firewalls has achieved significant success in reducing the incidence of effective hacks. Unfortunately, the architecture required for such devices and techniques tends to provide network bottlenecks that are natural targets for sophisticated denial of service attacks.

Event logs and automated tools to facilitate recognition of bad acts was the stalwart of detection mechanisms until the recent widespread implementation of intrusion detection systems (IDS). To be effective, existing monitoring mechanisms must record a large volume of raw data for analysis. For example, a network IDS may record every transmitted packet, while a host monitoring system may need to record every user keystroke.

The ability to establish user accountability is fundamental to protection strategies. To protect computer networks, it is always helpful, and frequently essential, to be able to attribute specific activity to a specific end user. To ensure that this capability is available when it is needed, it may be necessary or desirable to attribute every action on the network to the appropriate end user. As we shall discuss later, this clearly has implications on the privacy of end users.

3 Privacy and Accountability

3.1 Privacy

We use the term privacy to represent personal privacy, as opposed to the more common, and narrower, interpretation of confidentiality. Essentially, privacy means controlling all information about oneself, including protecting identity (anonymity), personal information, and information about personal activity. This includes having the ability to disclose personal information to selected parties, while preventing disclosure to other parties.

The ability to protect one's identity has received increased attention since the advent of the Internet. As a result of the Internet's powerful search capabilities and ability to dig up personal information, masquerading has become a real nuisance, if not a major threat to the Internet itself. Here we see a connection between authentication and privacy: being able to identify oneself is a matter of authentication, while preventing others from assuming your identity or from authenticating you without your approval is a matter of privacy.

Lastly, users often desire to hide their activities on the network. For example, a user may desire to access Internet services without allowing anyone (or preventing only specific parties) to know that she accessed the service. Three seemingly legitimate instances where users may desire anonymity include: (a) the ability of a potential customer to window shop electronically without the shop knowing the information she has gathered about competing products (b) where an employee may not want his boss to know that he has been accessing employment services web sites, and (c) decision-making processes where ideas are intended to be judged based on their merits rather than on their originators.

3.2 Accountability

Accountability is the ability to attribute actions to the user that caused those actions. It seems only possible if users can be accurately authenticated. Authentication has been the topic of extensive research, mostly focused on cryptography as the enabling technology. Passwords are the de facto authentication standard, though they provide only weak guarantees of authentication.

Recently, authentication using public key cryptography has received much research attention. Cryptography has broad power and flexibility in solving multiple security problems, including privacy, integrity and non-repudiation, as well as authentication. Our ability to apply cryptographic methods to the authentication problem rests with the infrastructure that is established to handle the myriad required functions. The foundational components of this infrastructure are security protocols that apply cryptographic tools [15].

Public key infrastructures (PKIs) have been proposed and partially deployed as a method for facilitating authentication in security protocols. However, there have also been advisories issued about the risk of such infrastructures if they are oversimplified (see e.g. [5]). Nonetheless, because of their architectural position between the end user and the actions taken by, and on the behalf of, the users, PKIs and related security protocol infrastructures offer an excellent environment that can balance accountability and privacy concerns when properly implemented. An important focus should be to develop cryptographic infrastructure models, techniques, principles, and tools to facilitate accurate, efficient, privacy-balanced accountability.

To complement authentication methods, efforts should be made to investigate policies, tools, and techniques that will facilitate accountability during system operation. Authentication in itself does not ensure accountability. Results must be traceable to action originators when necessary as a response to particular events.

Finally, current research on cyber-forensics focuses on how to use current and emerging technologies to extract information, e.g. by wiretapping, confiscating computers, using hysteresis properties of magnetism to recover erased data. We must also explore *before-the-fact* policies and procedures that will facilitate system analysis *after-the-fact*. Techniques perfected for forensics applications must be combined with management policies and practices to give a level of accountability and a manner of situational awareness to privacy issues that are not presently possible by addressing operational policies and their impact on cyber-forensic efforts.

Cryptographic methods can also be used to extend cyber-forensic capabilities by assisting investigators at reconstructing elements of an intrusion, while protecting such information in the typical, non-intrusion case. This technology is based on research on copyright techniques (see e.g. [2,1,9]) that focuses on using special encoding (as encryption) to enhance tracing of copyright violators.

3.3 The Privacy Dilemma

Keeping a balance between the conflicting rights of different parties seems almost impossible. However recent research on some of the more acceptable forms of key escrow has shown that it is possible to deal with conflicting requirements in a “fair” or “equitable” way using cryptographic techniques (see e.g. [3,6]).

To properly analyze the requirements of accountability and privacy, one must understand and balance the rights of the individual and the needs of society. In particular, it is important to consider the conflicts between:

- (a) Anonymity and accountability,
- (b) Privacy and authentication,
- (c) Privacy and cyber-forensics,
- (d) Free speech and liability/copyright.

As noted earlier, the concept of privacy includes protecting knowledge of one's actions. Activity protection is commonly accomplished through anonymity. Unfortunately, anonymity undermines, to a certain extent, the protection goal of accountability; that is, it may be that bad acts accomplished by anonymous entities cannot be deterred by retribution. On the other hand, as we discussed before, there are scenarios where anonymity is desirable or even necessary. Clearly, anonymity and accountability both have a place in networks, and balancing their conflicting characteristics will require significant effort.

Another easily recognizable conflict is between privacy and authentication. Once identity is divulged for authentication, the ability of users to control all aspects of their privacy is reduced. One option to protect privacy is not to allow oneself to be authenticated. Unfortunately, authentication is a fundamental element of many network activities. Access control typically requires some form of authentication. If a user wants to store information on a network and to protect that information from general access or manipulation, he must be able to distinguish himself as the information owner, or at the very least present some credential indicating authority to access the information. A similar conflict occurs with voting systems and auction systems.

Cyber-forensics techniques are frequently at odds with privacy considerations as well. At the core of cyber-forensics techniques is finding the identities of those responsible for action. Moreover, it is also important to identify exactly when the action occurred, why it was taken, what the goal of the action was, and so on. A cyber-forensics expert seeks to know every detail about every aspect of every principal under investigation. Thus, the goals of privacy are apparently in direct conflict with the goals of cyber-forensics.

Finally, we recognize a natural conflict between allowing free speech and enforcing copyright and liability laws. For example, the owner of a Web page wants free speech but may be liable for the content. In some countries, such as Germany and Britain, Internet Service Providers have decided, on their own, to censor controversial Web pages, an overly simple solution to solving this accountability problem that leaves users unable to communicate privately. Findings of an earlier National Security Council study reflect similar tradeoffs between authentication and confidentiality: [13]

“The committee emphasized the importance of authentication (over confidentiality) for both technical and policy reasons. The technical reason is that authentication is the first line of defense against the most serious threats to NISs [Network Information Systems] for critical infrastructures-intruders attempting to deny the benefits of using NISs to authorized users.”

4 Balancing Security and Privacy

4.1 Accountable Privacy

We propose that the overarching goal for addressing the conflicting requirements of accountability and privacy discussed in Section 3.3 must be to: (a) identify the guilty and, (b) protect the innocent. We coin a term to address this easy to say, yet hard to accomplish concept: *accountable privacy*. We posit that it should be possible to enable users to maintain a reasonable level of privacy as long as they do not abuse the privilege. Specifically, we seek tools that will allow decision makers to evaluate the quantitative meaning of the reasonable level of privacy and what constitutes abuse.

To balance the requirements of protection against those for privacy, one promising direction is to investigate methods to facilitate and expand distributed computing capability through advanced accountability technology. Cryptographically oriented infrastructures, similar to public key infrastructures (PKI), are a proven mechanism for accomplishing both security and privacy goals. There is extensive existing research in cryptography, security protocols, and PKIs that, when coupled

with new models, methods, and techniques can provide accountability and preserve functionality while concurrently balancing security with needs for privacy.

4.2 Models for accountable privacy

Good models are an important tool to describe problems and their solutions formally. For each desired property of accountable privacy a model will be necessary. For some properties such as privacy, we already have a model: Shannon's secrecy model [11], which is based on probability theory. Other models are based on computational complexity and logic. However, not all properties of accountable privacy have been formally modeled as yet. The work of Millen and Wright [10] is a useful starting point for addressing liability.

Shannon's secrecy model is based on probability theory. Other models are based on computational complexity or logic. Although early research with computational complexity models led mainly to impractical schemes, recently several practical protocols have been proposed. One should therefore investigate models based on all three approaches: probability, computational complexity and logic.

4.3 Enhancing accountability

Accountability is presently accomplished by a combination of: (a) authentication, (b) action/event binding, and (c) monitoring.

(a) *Authentication Methods*: Identity may be traced from an IP address, to a pseudonym, to an account name, to the registered name at the ISP, and often through other identifying stages, eventually to some fundamental, identifying information, such as a social security number, a finger print, or possibly a DNA match. An important characteristic of authentication is the degree of confidence that can be achieved. Traditional methods depend on rigor and heuristics to show that authenticated mappings are accurate. Another research direction addresses authentication methods based on *interactive zero-knowledge proofs* [7].

(b) *Binding Actions to Events*: Few mechanisms for binding action to events have been proposed, and indeed, when such mechanisms have been engineered into the infrastructure, public outrage has purged them from the marketplace, e.g. Carnivore and Clipper. On the other hand, many commercial and public domain mechanisms were developed using operational information (for example information included in a message that allows a response) to trace events to the action that caused the event, and to bind the root actions to an end user. Forensics tools have come a long way in the past five years. However, there is still more to be done, particularly to find tools that properly balance accountability with privacy.

(c) *Monitoring*: To ensure accountability, monitoring must be feasible and effective. Tracing all packets on the Internet leads to such massive data that the result would be too large for even the most sophisticated data mining techniques to analyze. On the other hand, tracing too little activity leads to insufficient information to identify and prove the guilt of attackers, since large efforts are sometimes required to know the identity of a message originator. Despite the fact that legal actions have sometimes been taken, it is clear that hackers are not deterred. The amount of effort required to trace perpetrators, plus the effect on the efficiency of the network, must be weighed against the effectiveness of doing so.

4.4 Survivability

The reliability of a network, i.e., the survivability of a network even in the face of malicious attacks, is often more important than tracing an attacker. For example, an issue that has received quite some attention is the fact that our critical infrastructures (such as the food and water distribution, etc.) are very dependent on computer networks (see http://www.ciao.gov/PCCIP/PCCIP_index.htm). In the case of an electronic Pearl Harbor, it is more important that the computer network remains sufficiently reliable. For critical network activities, the issue of being able to trace those who attacked is important but obviously secondary to the survival of the network in the face of attacks.

5. Conclusion

It seems that without the ability to monitor activity, we cannot ensure accountability. Therein lies the rub. Monitoring, surveillance, oversight, listening devices, security cameras and spy cams, all illicit shudders from those that have experienced the draconian *Big Brother* policies of extremist military states. While privacy is not mandated within the US constitution, clearly freedom is not possible without privacy. Neither is freedom possible without protection.

On September 11, 2001, the United States suffered the worst instance of terrorism in its history. It has been claimed that this action was possible in part because we have not established an operational balance between privacy and protection. In testimony before congress in June of this year, the FBI Director stated: [8]

"Uncrackable encryption is allowing terrorists – Hamas, Hezbollah, al-Qaida and others – to communicate about their criminal intentions without fear of outside intrusion. They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

In order to preserve and affirm the liberties and freedoms that are at the core of our society it is therefore essential that we form a nucleus of new models, concepts, policies, tools, and techniques, to balance privacy and accountability. In a democratic society we must be able to speak freely, yet not be able to shelter threatening or deadly communications from proper authorities. At the same time, citizens should be able to adequately protect themselves, even from their own government should democracy dissolve or be overthrown. We must be able to move about freely without our every move tracked by a big brother, yet not be able to hide malicious actions from investigators as long as our society remains democratic (see [3,6]). We must have reasonable access to goods, services, and information while protecting the rights of producers to earn a fair profit.

Finally, we contend that the slow progress of research on accountability, privacy, and indeed security are partially attributable to our lack of focus at the highest levels. This is highlighted by the following excerpt from a document written by the President of the National Academy of Engineering:

"I am deeply troubled, however, by a deeper issue. There is virtually no research base on which to build truly secure systems. For historical reasons there has been no federal funding agency that saw itself as responsible for supporting research in this area – not DoD/DARPA, not NSF, not DoE, not NSA. The absence of a lead funding agency that felt it "owned" this problem has led, I believe, to tentative, incremental research that did not question its underlying assumptions – assumptions that are grounded in the 60's mainframe environment." [14]

Now is the time to set a course to establish a framework and the inner-workings to provide accountable privacy. We may need an agency that is designated to take the lead to establish a coordinated plan to improve and expand, but not restrict, security and privacy research and

technology directions. Once this technology is in place, value decisions regarding privacy policies can be made by policy setters based on the best means for achieving the desired functionality, rather than being limited by the lack of options that presently exist.

References

- [1] D. Boneh and M. Franklin. An efficient public key traitor tracing scheme. *Advances in Cryptology Crypto '99, Proceedings, LNCS 1666*, Springer, Berlin, pp. 338-353, 1999
- [2] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *Advances in Cryptology Crypto '95, Proceedings, LNCS 963*, Springer-Verlag, pp. 452-465, 1995.
- [3] M. Burmester, Y. Desmedt and J. Seberry. Equitable key escrow with limited time-span. *Advances in Cryptology, Asiacrypt 98, LNCS 1514*, Springer, Berlin, pp. 380-391, 1998
- [4] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *Advances in Cryptology, Crypto '98, Proceedings, LNCS 1462*, Springer-Verlag, pp. 13-25, 1998
- [5] Carl Ellison and Bruce Schneier. Ten Risks of PKI, What You Are Not Being Told About PKI. *Computer Security Journal*, Vol. XVI, No. 1, 2000
- [6] Y. Desmedt, M. Burmester and J. Seberry. Equitability in Retroactive Data Confiscation versus Proactive Key Escrow. 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC2003, *Proceedings, LNCS 1992*, Springer-Verlag, pp 277-286, 2001
- [7] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1), pp. 186-208, 1989
- [8] Jack Kelley. Terror groups hide behind Web encryption. *USA Today*, June 19, 2001, <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm>
- [9] K. Kurosawa, T. Yoshida, Y. Desmedt, and M. Burmester. Some Bounds and a Construction for Secure Broadcast Encryption. *Advances in Cryptology, Asiacrypt 98, LNCS 1514*, Springer, Berlin, pp. 420-433, 1998
- [10] J. K. Millen and R. N. Wright. Reasoning about Trust and Insurance in a Public Key Infrastructure. *Proceedings of 13th IEEE Computer Security Foundations Workshop*, IEEE Computer Society, July 2000
- [11] C. E. Shannon. Communication theory of secrecy systems. *Bell System Techn. Jour.*, 28, pp. 656-715, October 1949
- [12] Donald Rumsfeld. US Secretary of State, Comments to the press, Sept 12, 2001, http://www.defenselink.mil/cgi-bin/real_audio.pl?Sep2001/DoD091201a&1000322100
- [13] Fred B. Schneider. *Trust in Cyberspace*. National Academy Press, p. 214, 1999
- [14] William A. Wulf, Transcript of Letter to Dr. John Hamre, Director, Center for Strategic and International Studies, July 2001
- [15] Alec Yasinsac and Wm. A. Wulf, "A Framework for A Cryptographic Protocol Evaluation Workbench", to appear in *The International Journal of Reliability, Quality and Safety Engineering (IJRQSE)*, Sept 2001