Expressing and Enforcing Robust Behavior for Electronic Objects

Sean W. Smith
Computer Research and Applications Group (CIC-3)
Los Alamos National Laboratory

Los Alamos Unclassified Release LA-UR-97-1705

May 16, 1996

Abstract

The rapidly changing and expanding electronic environment is fundamentally different from anything mankind has previously experienced. The challenge of information surety is to assure that computation and information behave reasonably and predictably – despite malice, failure and human nature – in this hostile and dynamic environment. Addressing this challenge is urgent for national and economic security, but requires both the ability to express the necessary robustness properties for electronic objects, as well as the ability to develop technology to achieve these properties. This position paper expands on these problems, and presents some solution strategies.

1. The Problem

An aphorism that we often need to repeat is "the electronic world is not the same as the physical world." Securely moving physical and paper-based processes into electronic settings requires understanding which behaviors and metaphors still apply—and which ones change. As more commerce and service applications migrate to the Internet, the lack of this understanding will lead to security and privacy weaknesses in these services. Future research needs to address this knowledge gap.

Humanity has had millennia to develop an understanding of how paper works: what properties it possesses innately, what additional properties it needs (in order provide secure foundations for higher-level applications), and what controls and techniques can be used to grant it those properties. To secure our electronic future, we need to develop similar understanding, definitions, and techniques for the emerging electronic environment.

- Who should be allowed to do what with computational entities?
- How do we express these rules?
- How do we enforce them, both in the current and in the emerging computational base?
- What fundamental constraints does technology introduce?

We, as a society, base our intuitions and craft our policy and law on the frequently implicit constraints of paper. The mismatch between this intuition and new electronic world, freed from these constraints, leads to security risks. Addressing these issues require both technical research, as well as increased education and awareness among the user and designer community.

This is a Latex/postscript version; pagination may differ from the original paper version.

2. Examples

Even the basic example of digital signatures illustrates why this is a difficult and poorly defined problem. Salesmen for the Information Age tout that digital signatures are superior to their physical counterparts, because a digital signature depends on each bit of the document in question. While this claim is true, it is also true that unlike their physical counterparts, digital signatures face significant threats to their long-term validity. These threats include the gradual progress of computation, as well as potential breakthroughs in factoring (e.g., [15]), computer technology (e.g., [19]), or understanding of hash functions (e.g., [8]). In contrast, no foreseeable technological development will render invalid John Hancock's signature on the Declaration of Independence.

However, more subtle and serious issues abound.

Electronic implementations can overlook critical properties of physical objects. For example, physical cash possesses a number of robustness and anonymity properties which are often absent in electronic versions. [3]. Even the pioneering DigiCash electronic cash protocol [5] fails to incorporate the basic property of transactional atomicity (i.e., the action happens entirely or not at all). [25] When Alice gives a physical dollar bill to Bob, then Alice has the bill until Bob does; even in failure scenarios, exactly one dollar bill exists—money is neither created nor destroyed. However, when Alice gives a digital dollar to Bob, failure scenarios exist where the ownership and existence of the dollar is ambiguous. Nevertheless, once noted, this problem can be resolved. [4]

However, electronic environments can make it impossible to reproduce basic properties of physical services, even if proposed implementations explicitly acknowledge these properties. For example, physical postmarks are valid indefinitely, can be verified without consulting a central archive or authority, and cost \$0.32. This set of properties cannot be achieved in an electronic version. Because of the intractability assumptions that underlie current cryptography (advances in computation and/or understanding of the complexity foundations can render current cryptosystems invalid), electronic postmarks must either use an archive and sacrifice independent verifiability (e.g., [17]), or use cryptography and sacrifice indefinite validity. (The technique of "renewing" timestamps (e.g., [12]) can mitigate the finite lifetime of cryptography, but this is notion is foreign to the paper world.) Additionally, services such as electronic postmarks exhibit a phenomenon of amplified consolidation [22] which produces a market whose equilibrium price converges to the incremental cost of "stealing" a service—so it is also not clear whether the price of the paper analog will apply in the electronic world.

Furthermore, the power of new electronic settings complicates older approaches to access control—compare what Bad Bob in New York City can do in fifteen minutes today, versus what he could do in fifteen minutes fifteen years ago. The rules of legitimate data access need to change when the environment can greatly amplify the magnitude of user access, since sufficiently many individually legitimate queries may, collectively, constitute illegitimate activity. The recent compromise at the Brooklyn Social Security office [23] may illustrate this problem: one insider made $10,000$ queries, each one of which may have appeared legitimate. The worlds of classified and commercial data access also provide examples of this problem. Minimally, it seems that whether agent X should have access to data item Y should depend not just on a fixed table entry, but be functionally determined by the context of the access.

Indeed, the whole concept of publishing and intellectual property protection changes when the medium becomes electronic. The packaging of a physical book or journal enforces implicit license agreements: the owner can read specific articles and can lend the book to a friend, but cannot copy the work, cannot effectively timeshare a single copy with 100 friends, and cannot repackage the material in another work. On its own, the electronic medium enforces no such copy, access, and redistribution restrictions. The malleable nature of electronic media also complicates other traditional approaches to paper publications. For example, electronic typesetting permits easy revisions; how can policy crafted for the typewriter age apply to an age where a "document" is a dynamic sequence of versions? How does an author fit a URL into a bibliographic entry—and what does the reader do when, six months later, that URL no longer is valid?

Migrating activity into electronic settings complicates notions of fairness and order. Distribution and failures complicates the notion of time as an ordering of events. [21] Distribution also complicates the notion of real time and duration—and making trading decisions electronically (instead of by humans) grants significant consequences to small differences in relative communications time. [2]

The electronic environment also complicates the notion of authenticity. To quote a New Yorker cartoon, "on the Internet, no one knows you're a dog." Who or what is really on the other end of a connection? This standard authentication problem can surface in subtle ways. For one example, building a fake ATM is sufficiently difficult that the primary successful instance is well-known. [9] Building a fake ATM on top of a real ATM, that provides real service plus extra services, is much more difficult. However, building a fake Web site—wired to the legitimate site and providing some legitimate services, while also requesting extra information—is easy; the legitimate site provides the necessary graphics, and unfortunately (as Mike Neuman puts it) "users never look at the URL they click on."

Another set of authenticity challenges arises when considering the users of Web services. This new world places human users, legitimate automated tools, and tools of uncertain legitimacy all in the same environment, frequently indistinguishable from each other. For example, the existence of music vendors on the Web has given rise to the existence of music meta-vendors, who will take an order and shop for the best deal; many music vendors now attempt to block access of such meta-vendors. [26] A Web site offers free access to the Dilbert comic strip, but forces users to go through an advertising page before finding the randomized URL for the daily strip; it is rumored that students are constructing automated processes to visit the advertising page and report back with the Dilbert.

Yet another set of authenticity challenges arises when considering the use of smart cards and secure tokens to provide secure sub-environments. [11] Leaving the boundary of a secure subenvironment within an untrusted electronic setting exposes the secure subenvironment to the risk of unsecure input. For example, a PCMCIA card inserted into a laptop in a hotel room may provide a secure tunnel back home—but how does the tunnel distinguish between the user's keystrokes and a Trojan Horse simulating the user's keystrokes? For another example, a dishonest merchant may tell a customer one price for a book, but have his smart card reader tell a different price to the customer's smart wallet.

This list is incomplete, and intended only to illustrate the diversity of instances of this problem. (Unfortunately, the next two months of the New York Times and the RISKS Forum would undoubtedly provide a completely different set of examples.)

3. What Makes Electronic Different

Some researchers argue that the electronic world presents no fundamentally new risks, but only more instances of traditional risks. This paper takes the opposing view: the electronic world is fundamentally different. Securely migrating services into the Internet environment requires understanding this difference, since rules, custom, and policy crafted for the paper world will not always apply. Minimally, this mismatch can permit inventive adversaries to exploit and subvert these new services. But potentially, this mismatch could lead to significant information catastrophes. (For example, what if five years from now, our society systematically uses secure tokens to sign all legal documents, but five years later, it is revealed that all these tokens suffered from a vulnerability such as Kocher's [14] timing attacks?)

Electronic objects behave differently from paper, since they are free from the constraints that bind paper. What makes this challenge especially vexing is the fact that the paper constraints, upon which we rely, are often implicit and overlooked. Bits can be examined and copied without being disturbed (quantum cryptography aside), and cannot be dated or dusted for fingerprints.

Electronic processes likewise differ. Distribution in complex, failure-prone environments leads to unforeseen failure scenarios. Migrating services into electronic environments requires first mapping humans and human processes into these environments; this mapping creates the possibility for automated activity and attacks. The distribution and complexity of the environment permits remote and anonymous attacks. (Witness even the now-ancient phenomenon of "flaming" that emerged when humans were no longer directly connected to each other.) Both mechanical barriers and social barriers disappear.

Likewise, the electronic community differs. Connectivity leads to volatility; witness how quickly the World Wide Web exploded; how quickly S-HTTP vanished; and how quickly Java is emerging. The speed with which new attacks spread throughout the malicious hacker community forms a frequently-heard lament from security officers. The pace of change outstrips the evolution of social values; witness even the diversity of values among the alleged good guys. (For example, should the information age inherit the values of librarians, broadcast media, or public relations staff?)

Admittedly, the increased power of the electronic world is a two-edged sword, enabling new forms of defense as well as new forms of attack.

4. A Call for Research

One approach to addressing this challenge is research. Until we can understand how to express how electronic objects should behave, and how to force them to behave this way, we will continue to suffer from the security risks associated with scenarios in Section 2.

This section sketches our current research path: formalizing these problems, building proofs of concept to demonstrate what is achievable, and demonstrating theoretically the fundamental limitations.

4.1. The Greater Context

This proposed research does not exist in a vacuum. Much interesting and relevant work has been done addressing many instances of this problem. An incomplete list includes work in rights management (e.g., [24]), in new approaches to electronic publishing (e.g., [6]), in the wealth of new commerce and Internet payment initiatives (e.g., [7, 10, 16, 18, 20]), in migrating public sector services onto the Web (e.g., [1]), and even in the older problems of anomaly and intrusion detection (e.g., [13]).

However, these efforts are pieces of a still-incomplete mosaic: how to specify how electronic objects should behave, and how to enforce that behavior despite hostile environments and malicious players.

4.2. Expressing Robust Behavior

Solving a problem requires defining the problem. Consequently, one of the first steps in this proposed research should consist of developing a formal language in which to express the rights properties appropriate for electronic objects. To keep a pragmatic focus, this process should be informed by real problems (e.g., Section 2).

4.3. Enforcing Robust Behavior

Once some example security problems are extracted and placed them in a formal framework, research should explore what properties can be achieved (and what cannot be achieved) in current and in emerging computational environments. Our current work focuses on three models:

No Trust. The most pessimistic vision of globally distributed computing is much like today's Internet and academic networks: individual users have a small amount of trust in the integrity of individual machines, but no other security base exists.

Some Centralized Trust. A vision that more closely approximates the aspirations of many government and commercial players consists of an untrusted distributed base, with a small number of highly trusted nodes.

Distributed Trust. We suspect that many desirable surety properties will not be possible in the centralized trust model. The emerging technology of secure coprocessing (e.g., [25]) enables a computing base where small but

widely trusted computational nodes can be distributed throughout the environment. We see this model as a promising mechanism for addressing security and rights issues in distributed, open environments.

One needs a security foothold from which to bootstrap. Secure coprocessors—small but reasonably powerful (and inexpensive) tamper-resistant computational environments—can provide this foothold. Current smart cards (e.g., the chip card technology being deployed by Visa and MasterCard) provide a low-end example of this technology. However, higher-end coprocessors—in PCMCIA and other formats, and featuring more powerful environments—are emerging.

Adjunct to the development of formal methods and analysis of information objects is developing a framework for the intuitive understanding of information objects and spaces. Techniques adapted from the field of scientific visualization might lead to better intuitive understandings of information objects and spaces.

4.4. The Challenge

Only one portion of this proposed work will consist of applied development, and only a portion of that will target the distributed trust model that secure coprocessing enables. However, even the basic task of constructing a migrating, restricted-usage software entity running on PCMCIA-equipped workstations requires exploration of many critical issues:

Rights Management. How do we even express use limitations?

Algorithm Design. How do we partition the software's algorithm so that the portion running on the coprocessor remains secret?

Traffic Analysis. How do we construct the coprocessor's operating environment (e.g., its cryptopaging strategy) to minimize the information an adversary can learn?

Anomaly Detection. How does the coprocessor distinguish between communications from the legitimate user and communications from an adversary? How can the software's audit trails be usefully evaluated for anomalous or invalid behavior?

Information Hiding. How do coprocessors communicate to each other in a hostile environment? How can secured software objects leave tamper-resistant audit trails?

Information Visualization. What metaphors can be used to effectively understand a wide range of information objects and spaces?

4.5. Conclusion: a Call for Awareness

Electronic is different. Because of this difference, we need to understand how to express and enforce robust behavior for objects and processes freed from the inherent robustness of paper. Section 2 presented examples of how this lack of understanding causes problems, Section 3 presented some high-level arguments about the root causes, and Section 4 proposed a path of research. However, high-level arguments are often mistaken for hand-waving, and research, even when successful, can lead to unsatisfying results. This leaves us with the problem examples.

Hence, besides research in the academic and laboratory community, a second path toward addressing this problem is increased education and awareness in the communities of users, designers, and policy-makers. (Indeed, this paper and this work represent one step toward this vision.)

The greater picture which this paper sketches is ambitious, and contains the seeds for many projects and theses. (Indeed, even enumerating all existing relevant efforts constitutes a sizable project.) However, while our understanding, cultivation, and control of electronic objects is incomplete, our electronic future is at risk.

Disclaimers

Acknowledgments

The author is grateful to his colleagues—including Gary Christoph, Justin Doak, John Dragon, Vance Faber, Kathleen Jackson, Manny Knill, Rick Luce, Robin Morel, Steve Smith, Doug Tygar, and Bennet Yee—for their helpful advice and suggestions.

References

[1] S. Adelson, R. Rivenburgh, and S.W. Smith. *Enforcing Closure of Subwebs and Expansive Web Sites.* Los Alamos Unclassified Release LA- UR-95-4410. December 1995.

[2] M. Bigliardo, J. Fried, C. Schafer, S. Tisdale, and R. Torres. *A High- Level Protocol and System for Computer Controlled Financial Trading.* Information Networking Institute Technical Report TR-1993-9, Carnegie Mellon University. October 1993.

[3] L.J. Camp, M. Sirbu and J.D. Tygar. "Token and Notational Money in Electronic Commerce." *First USENIX Workshop on Electronic Commerce.* July 1995.

[4] L. J. Camp. *Reliability, Security, and Privacy in Electronic Commerce.* Ph.D. thesis. Engineering and Public Policy, Carnegie Mellon University. Draft, 1996.

[5] D. Chaum. "Security without Identification: Transadction Systems to Make Big Brother Obsolete." *Communications of the ACM.* 28:1033-1044. October 1985.

[6] B. Cox. "Superdistribution." *Wired.* September 1994.

[7] S. Crocker. "CyberCash: A Payment Infrastructure for the Internet." *Financial Services Technology Consortium Electronic Commerce Project Workshop.* October 20, 1994.

[8] H. Dobbertin. *Cryptanalysis of MD5 Compress.* Manuscript, May 2, 1996.

[9] "Fake ATM Machine Steals PINs." *The RISKS Forum.* Volume 14, Issue 59. May 11, 1993.

[10] Financial Services Technology Consortium. *Electronic Check Proposal: Public Document.* 1995.

[11] H. Gobioff, S.W. Smith, J.D. Tygar. *Smart Cards in Hostile Environments.* Los Alamos Unclassified Report LA-UR-95-2224. June 1995. Reprinted as Computer Science Technical Report CMU-CS-95- 188, Carnegie Mellon University, September 1995.

[12] S. Haber and W.S. Stornetta. "How to Time-Stamp a Digital Document." *Journal of Cryptology.* 3:99-111. 1991.

[13] J. Hochberg, K. Jackson, C. Stallings, J. McClary, D. DuBois, J. Ford. "NADIR: An Automated System for Detecting Network Intrusion and Misuse." *Computers and Security.* May 1993.

[14] P. Kocher. *Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks.* Extended abstract. December 7, 1995.

[15] A. Lenstra. "RSA130 is Completed." *RSA Factoring-By-Web: The World-Wide Status.* April 11, 1996.

[16] B.C. Neumann and G. Medvinsky. "Requirements for Network Payment: the NetCheque Perspective." *IEEE Computer Communications Conference.* March 1995.

[17] C. O'Hara. "USPS to Launch Electronic Postmarking." *Federal Computer Week.* May 6, 1996.

[18] T. Okamato and K. Ohta. "Universal Electronic Cash." *CRYTPO '91 Proceedings.* Springer-Verlag, 1992.

[19] P.W. Shor. "Algorithms for Quantum Computing: Discrete Log and Factoring." *35th FOCS.* 1994.

[20] M. Sirbu and J.D. Tygar. "NetBill: An Internet Commerce System Optimized for Network Delivered Services." *IEEE Computer Communications Conference.* March 1995.

[21] S.W. Smith. *Secure Distributed Time for Secure Distributed Protocols.* Ph.D. thesis. Computer Science Technical Report CMU-CS-94-177, Carnegie Mellon University. 173 pp. September 1994.

[22] S.W. Smith, V. Faber, J. Hall. *The Econometrics of Amplifiable Electronic Services.* Draft, 1996.

[23] "Social Security Info Used by Stolen Credit-Card Ring." *New York Times News Service.* April 6, 1996.

[24] R. Weber. "Digital Rights Management Technologies." Northeast Consulting Resources. Octqober 1995.

[25] B.S. Yee. *Using Secure Coprocessors.* Ph.D. thesis. Computer Science Technical Report CMU-CS-94-149, Carnegie Mellon University. May 1994.

[26] B.S. Yee. Personal communication, May 1996.