Securing Confidence With Data Escrow

Donna M. Schaeffer, Marymount University, USA
Patrick C. Olson, National University, USA

ABSTRACT

In the past several years, the general public has had concerns about hacking and identity theft. Headlines in news media include computer system breaches at popular and respected companies like Target and universities like The University of California at Berkeley.

This paper explores options available for providing the general public with the benefits of the information age while mitigating against the security risks. We begin with a discussion of it is reasonable for the general public to expect organizations engaged primarily in commerce to provide for their cybersecurity. We then look at how electronic transactions are currently secured. We conclude with a consideration of the "protocols" or "institutions" that might provide for security for consumers.

Keywords: Cybersecurity; E-Commerce; Data

INTRODUCTION

The terms "digital world" and "the information age" mean many different things to people, but the promise the terms hold is generally an improvement over current conditions. The shortcomings, e.g., identity theft, that many people experience from participating in the digital world or information age, can in no way be viewed as improvement. In this section, we define important concepts, provide examples of the impact on people and the public when shortcomings are manifested, discuss reasonable cultural expectations about security, look at how we currently develop e-commerce systems, and provide an alternative approach.

It is useful to reflect on the four terms that comprise the title of this work: securing, confidence, data and escrow. Securing means to protect against threats or to make safe. The general public wants their electronic transactions and records to be secure.

Confidence means the feeling or belief that one can rely on someone, or something or a firm trust. The general public will not use digital systems that they do not trust.

Data is distinct information that is formatted in a certain way. The general public has to have confidence that data in electronic records is secure.

Escrow is a bond, deed, or other document kept in the custody of a third party, taking effect only when a specified condition has been fulfilled. This concept becomes important because there are some transactions where none of the entities party to the transaction "own" the data. Yet that data is needed for the transaction to occur, and a third party aids the transaction.

The scope of allowing the general public to feel secure about digital transactions continues to grow. While once limited to the physical act of giving a credit card to a point of sale terminal in brick and mortar businesses, our digital transactions now take place in new ways and in industries that we may not have had transactions with in the past. Some examples include:

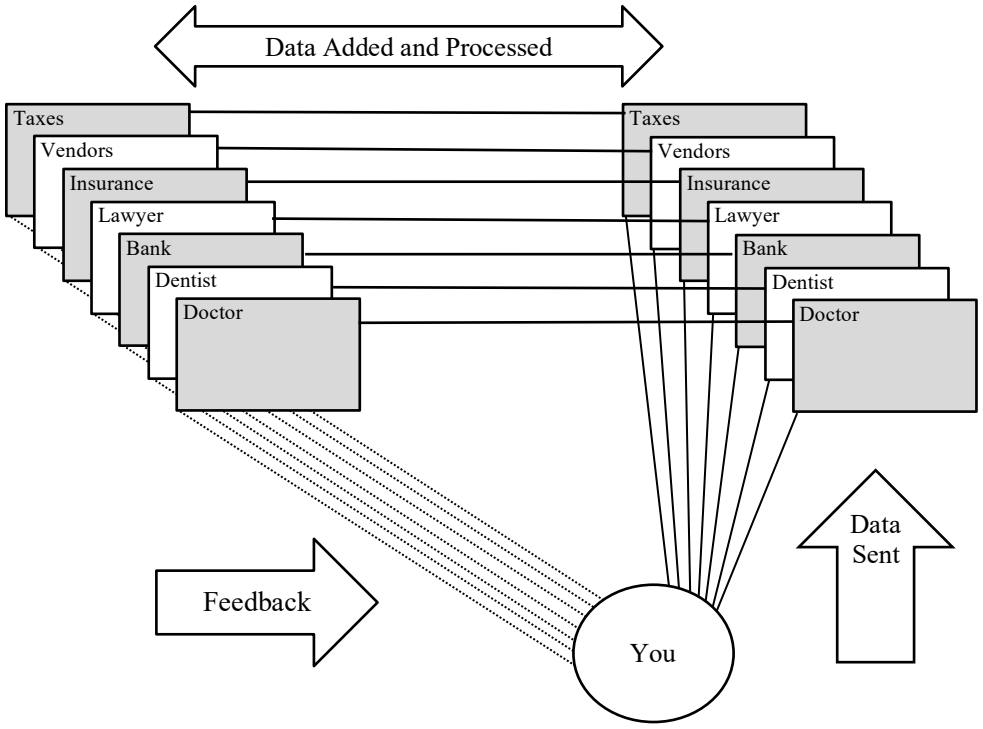
- Gaming: 11,266 log-in credentials were stolen from Microsoft Xbox users (Ellison, 2015).
- Dentistry: 151,626 patient records were stolen from the Advantage Dental group (Pamplin Media Group, 2015).
- Food service: an undisclosed number of debit/credit card information stolen from point of sale terminals at Bistro Burger (Greenburg, 2015).

Computer security breaches are so prevalent that the Privacy Rights Clearinghouse (2015) maintains a website dedicated to tracking breaches which are happening in almost every industry at what appears to be an increasing pace.

There is a great social need for secure transactions, and the general public has reasonable expectations that such transactions will be secure. This expectation may not be reasonable due to the scope of digital commerce. For example, by 2018 the web will account for 11% of retail sales. This is approximately $414 billion dollars (Forrester Research, 2014). Consumers between the ages of 25 and 33, i.e. Generation Y, spend more online than any other age group, with an average of $563 per individual in the first three months of 2014 (Forrester Research, 2014). Additionally, Generation X consumers, those between 34 and 47 years old, spent an average of $535 each online during the first three months of 2014 (Forrester Research, 2014). Ultimately, 69% of U.S. adults regularly buy online and purchase about 16% of their products online (Forrester Research, 2014).

Individuals engage in many different transactions in any given day. Any commercial transaction, for example buying a drink, involves at least a business process transaction at the point of sale. If the transaction involves a debit or credit card, there will be additional processes. The systems that manage each of these processes have been analyzed and built from a process-centric point of view. Even though transactions are a movement of data, the digital systems are almost always process oriented rather than data-oriented and are generally built from a client-server model. Figure 1 provides an abstract model of this type of system.

Figure 1. Process-oriented System



Failing to use a data-oriented approach may be one source of security problems. The figure shows that data is collected, moved, and processed to provide a service or good to "you", or the general public. Members of the general public will suffer if the data is mishandled, but likely have little or no access to the data.

The process-oriented model may inevitably lead to system security problems. Systems designed from this viewpoint are built to perform for the organization's interests, which may not be the same as the interests of the consumers they serve. As observed in Figure 1, "you", which represents the client or customer is outside the system boundary. Thus, even though all of these systems exist (at least in some sense) to support the "you" in the diagram, the "you" is not part of the system.

Thus, the "you" in the diagram is on their own. There is information about "you" everywhere, yet "you" have little or no control over that information and may not be able to compel the appropriate use and support of that information. In fact, "you" have no way to ensure that the information is even used properly for the immediate transaction, nor that it is being managed and stored for "your" best interests.

A SOLUTION: DATA ESCROW

An architecturally simple solution to this issue exists. The means of making sure all parties "get their due" from a transaction has been handled for many years in the financial industry by using escrow accounts. An escrow account is a contractual codification of what each party is entitled to and a specific description how the transaction works with a third party (in the financial industry the third party is a bank), acting as the independent entity that proctors the transaction. Most people who have purchased a house have experienced escrow. For example, a down payment may be held in escrow until a loan is secured. An escrow account may also be used to accumulate money for property taxes or homeowners' insurance as the buyer makes their monthly mortgage payments so annual transactions occur seamlessly.

For computer systems, the concept of escrow has been applied over several decades. As early as 1985, a law journal article discussed source code escrow (Pappous, 1985). Source code was placed in escrow to give the customer a safeguard against the various problems that the vendor might encounter as a company. In effect, if the vendor company were to go out of business, the customer was to get a copy of the source code

Frankel and Young (1995) provide an interesting examination of the use of standards and hardware to provide escrows. The Escrow Encryption Standard (ESS) is implemented in hardware as a "Clipper" chip. The United States government funded research and development, with the goal making communications more secure. A number of important questions related to the strength of the algorithm, management of keys, and even use of specific data fields raise concerns about this approach and the conclusion is that the system was too complicated. Additionally, for the Clipper Chip to be successful, a trusted "organization" was necessary, and this never evolved.

Computing technology can improve the escrow process, but it is not without difficulties. For example, what happens if one of the parties to the escrow agreement loses their key? In a physical system, the loss of a key can be addressed in a variety of ways. Denning (1996) studied 29 key escrow systems or approaches. Only five seem to have no data recovery approach. It seems that the issue of losing a key can be resolved.

The pervasiveness of digital systems brings important security concerns. For example, the exponential growth in data mining yields important privacy considerations and digital payment systems are intended to be a major paradigm shift for privacy throughout the world (Jarecki, Patrick, & Shmatikov, 2003). The proposed solution is to move the responsibility for the key from the analysts to the "data generator" (also known as the user or the you in Figure 2). This user "pre-negotiates" the ways an analyst can access the encrypted data.

The recent media attention to Facebook and Cambridge Analytics underscores the concerns. Many marketing data mining operations monitor users' activities and provide predictive information. When users receive banner ads or emails that says something along the lines of "if you liked product x you might consider these other products" data mining has produced that message. Some may not consider this a "privacy" issue, thinking it similar to stopping at the same coffee shop each morning on the way into their office building where the barista greets them by name and starts preparing their "usual" order.

Human actors have roles in both the way digital systems currently operate and in Data Escrow systems. The goal is not to be completely automated. Giving the user responsibility for their own escrow keys should facilitate user buy in, but it is not known if these users would have more confidence in the system.

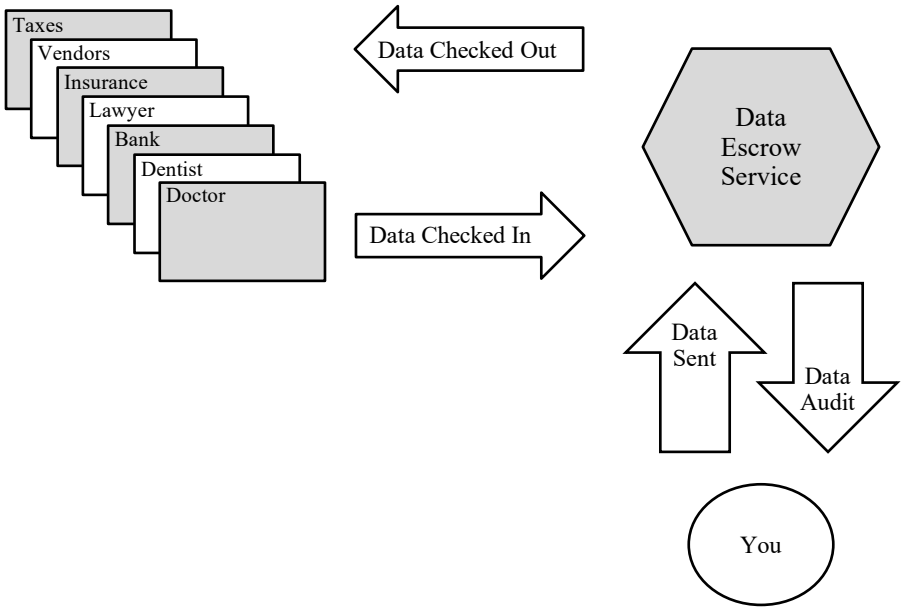
Ables and Ryan (2010) consider the interrelationship between societal security and individual privacy. Their orientation is that this interrelationship has "growing tension." It must be noted that they are in the United Kingdom where government data collection is more open, noticeable, accessible and perhaps more extensive that what is experienced in other parts of the world. This yields an interesting question: how should data be managed when societal security needs have been met? Ables and Ryan (2010) recommend that data is held in escrow and call for the development of a means to track and approve the use of the data. This involves "digital envelopes" and the use of the Trusted Platform Module. They suggest that, in their case, the government of the United Kingdom act as the operator of the escrow system, since they are the collector of the data.

Data Escrow could resolve the issues of confidence, privacy, and security. People have trust or confidence in the financial system's use of escrow, and these feelings may translate to Data Escrow. There is a societal expectation that the "you" which originates data have a reasonable right to the privacy of that data. It is also reasonable to expect that data about individuals are communicated and used in a secure and responsible way. Finally, it is reasonable for us to expect government use of data will protect both society and the individual.

Figure 2 illustrates the workings of a Data Escrow system. The Data Escrow service would be provided by an organization with attributes similar to a central bank. Its purpose is to operate the means of exchange for data via means similar to a central bank's work with money. The perspective of this system is an overview from the perspective of both end users and stakeholders. While it may look simplistic, the result should be an advance over our culture's current practices. The end user that is the subject of the data would be able to view, review, use and very importantly reuse both the data they provide and the data that is produced about them.

For organizations that produce data as a work product, a Data Escrow system could provide a greater access to temporal data (e.g. data that has been produced about a subject over time) and very likely a simpler means of restoring lost data in the event of a server or other problem. These and other improvements seem likely with an approach that focuses on providing a reliable system for data.

Figure 2. Data Escrow System



Current protocols, such Secure Socket Layer (SSL), Trusted Platform Module (TPM), and Escrowed Encryption Standard (EES) provide data protection. These protocols could be integrated in a Data Escrow architecture, and new standards could be introduced by professional associations.

At present, IBM and the Internet of Things (IoT) Foundation (Claburn, 2014) have expressed interest in Data Escrow. Several companies offer data and technology escrow. One example is Iron Mountain, which provides source code and Data Escrow services to over 94% of the Fortune 1000 (Iron Mountain Incorporated, 2015).

CONCLUSION

Data Escrow has two aspects that differ from other computing systems. One is the idea of a system for the "culture" or public. Typically, systems are built for specific circumstances and uses. Thus, when these systems are looked at in aggregate they appear, in a more generic cultural context, to disregard the needs of the "true" end users or the "you." The second aspect of Data Escrow is that there needs to be a social guarantor. That is, for the "true" end user, or the "you," to benefit from the expected utility may require a third partly to insure this result. To that end, we believe Data Escrow meets all needs.

AUTHOR BIOGRAPHIES

Donna Schaeffer, Ph.D., is a Professor in the School of Business Administration at Marymount University in Arlington, VA. She earned her Ph.D. in the Management of Information Systems at Claremont Graduate School. Dr. Schaeffer has participated on the Internet Advisory Caucus for the U.S. Congress, the Women's High-Tech Coalition, and the Business Advisory Forum of the United Nations. She has published over 100 articles and book chapters. Dr. Schaeffer serves as Director of the Doctorate of Science in Cybersecurity program at Marymount University.

Patrick C. Olson, Ph.D., is currently a Professor of Computer Science and Information Systems at National University. He earned his PhD in Management of Information Systems at Claremont Graduate University in 1999. He has an MS from USC in Systems Management. His undergraduate degree is from the University of Montana. He has been CIO at Menlo College where he developed, directed, and implemented enterprise-wide IP Telephony in 2000. He has held faculty positions in MIS at the University of Nevada and Cal Poly, Pomona. He started his career in the data center at Hughes Aircraft Company.

REFERENCES

Ables, K., & Ryan, M. (2010). Escrowed data and the digital envelope. In A. Acquisti, S. W. Smith, A.-R. Sadeghi, & Editors, *Trust and Trustworthy Computing* (pp. 246-256). Berlin, Germany: Springer Berlin Heidelberg.

Claburn, T. (2014, October 21). *IBM lays Internet of Things Foundation.* Retrieved from Informationweek: http://www.informationweek.com/cloud/platform-as-a-service/ibm-lays-internet-of-things-foundation/d/d-id/1316796

Denning, D. E. (1996, March). A taxomony for key escrow encryption systems. *Communications of the ACM, 39*(3), 34-40.

Ellison, K. (2015, April 3). *US teen pleads guilty to $100 million gaming hack*. Retrieved from WeLiveSecurity: http://www.welivesecurity.com/2015/04/03/us-teen-pleads-guilty-100-million-gaming-hack/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29

Forrester Consulting (2014, January). *Customer desires vs. retailer capabilities: Minding the Omni-Channel Commerce Gap*. Retrieved from SupplyChain247: http://www.supplychain247.com/images/pdfs/Accenture-hybris-Forrester-new_2014.pdf

Frankel, Y., & Young, M. (1995). *Proceeding of the 15th Annual International Crytography Conference: Escrow encryption systems visited: Attacks, analysis and design,* (pp. 222-235). Santa Barbara, CA., USA: Springer-Verlag.

Greenburg, A. (2015, March 16). *Malware installed at California burger joint, payment cards at risk*. Retrieved from SC Magazine For IT Security Professionals: http://www.scmagazine.com/malware-installed-at-california-burger-joint-payment-cards-at-risk/article/403762/

Iron Mountain Incorporated. (2015, October 31). *About us*. Retrieved from Iron Mountain: http://www.ironmountain.com/Company/About-Us.aspx

Iron Mountain Incorporated. (2015, October 31). *Historical milestones*. Retrieved from Iron Mountain Incorporated: http://www.ironmountain.com/Company/About-Us/Historical-Milestones.aspx

Jarecki, S., Patrick, L., & Shmatikov, V. (2003). Negotiated privacy. In P. S. Okada (Ed.), *Software Security - Theories and Systems - Mext-NSF-JSPS International Symposium, ISSS 2002 Tokyo, Japan, November 8–10, 2002,* (pp. 96-111) Revised Papers. Tokoyo, Japan: Springer Berlin Heidelberg.

Pamplin Media Group. (2015, March 16). *Advantage Dental says patient records were breached*. Retrieved from Portland Tribune: http://portlandtribune.com/pt/9-news/253880-123802-advantage-dental-says-patient-records-were-breached

Pappous, P. A. (1985). The software escrow: The court favorite and bankruptcy law. *Santa Clara High Technology Law Journal* ,309-326.

Privacy Rights Clearinghouse. (2015, August 19). *Chronology of Data Breaches*. Retrieved from Privacy Rights Clearinghouse Empowering Consumers. Protecting Privacy: https://www.privacyrights.org/data-breach