The Challenge of Data and Application Security and Privacy (DASPY): Are We Up to It?

Ravi Sandhu
Institute for Cyber Security
Univ of Texas at San Antonio
San Antonio, TX, USA
ravi.sandhu@utsa.edu

ABSTRACT

This talk gives a personal perspective on the topic area of this new conference on data and application security and privacy, the difficult nature of the challenge we are confronting and possible research thrusts that may help us progress to an effective scientific discipline in this arena.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—Access controls; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—Unauthorized access

General Terms

Security, Privacy

Keywords

Data and Application Security and Privacy

1. INTRODUCTION

It is a privilege and honor to start this new conference on data and application security and privacy (DASPY), in collaboration with my colleague and co-founder Elisa Bertino as well as the numerous volunteers who have worked hard to put it together. Before launching into a formal proposal to establish this conference, both of us chatted informally with various colleagues. Their unqualified enthusiasm for a high-quality research forum on this topic motivated us to push ahead. The response from the research community in terms of submissions and the caliber of the resulting program has been truly gratifying, confirming our intuition that this new conference serves a real need.

The term data security has been used for over three decades [2, 3, 8]. The connotation of privacy as an element of data security has often been emphasized [3]. Many of the fundamental problems and solution approaches were identified early on, such as the confinement or covert channel problem [10], statistical inference [6] and the promise of homomorphic encryption [12]. The general understanding of the term data security and privacy is probably not significantly changed since these early days, although of course in the details and nuances there have been considerable advances.

The term application security on the other hand has been and continues to be more amorphous. There isn't much usage of this term in the literature until relatively recently. In the past decade it has become a popular term but in a very narrow sense. For example, it has been equated to a subset of the more general term software security specifically applying to "protection of software after it has been built" [11]. In industrial practice this equates to scanning applications for vulnerabilities before deployment or filtering activity with application firewalls that detect or prevent application-layer attacks. This is particulary so in context of web application security [7, 13].

The intent of this conference is to use the term application security in a much broader sense. The connotation of the narrow sense of application security given above is that the application developer understands the security controls that the application should be enforcing but enforces them incorrectly by focussing entirely on functional aspects. Attackers are able to circumvent this enforcement by exploiting techniques such as SQL injection and cross-site scripting [14]. The much bigger challenge in application security is to understand what security policies need to be incorporated into the application logic. Of course, we still need to understand how these application-layer policies can be correctly coded so that we have high assurance that they cannot be bypassed. In other words the problem of software security is the how part of the problem of application security. This makes software security (i.e., how) a subset of the bigger problem of application security (i.e., what and how).

Is the what question really that big a deal? I definitely think so. Web applications deployed in the past decade have been e-commerce or e-business applications where the security policy of each individual transaction is fairly straightforward. Hence, industrial practice and consequent security breaches in this arena have been dominated by the how aspect. As we look to the future we anticipate the emergence of new applications wherein the what question is not going to be that straightforward. We are already seeing this in social networking, secure information sharing, secure collaboration, secure data provenance, electronic health records, location-based services, secure smart grid, and similar emerging applications. In these applications the security and privacy requirements are not at all obvious. It is a major research challenge to discover, articulate and formulate these requirements.

To summarize, the scope of data security and privacy has been fairly stable over the past three decades although many challenging research still remain. Usage of the term application security has become prevalent only in the last decade. Thus far it has been primarily used in the narrow sense of software failure to enforce fairly straightforward e-commerce and e-business policies due to unforeseen errors in how the security controls were coded. As we look ahead the challenge of securing emerging new applications is going to be driven as much or more by the what question rather than the how question.

CODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.
ACM 978-1-4503-0465-8/11/02.

2. THE DASPY SYSTEM CHALLENGE

Now that we have clarified the terms used in the DASPY topic we can turn to consideration of the DASPY system challenge. The essence of this challenge was actually articulated long ago as follows.

> "Generally, security is a system problem. That is, it is rare to find that a single security mechanism or procedure is used in isolation. Instead, several different elements working together usually compose a security system to protect something." [5]

Simply stated, the DASPY system challenge is how to develop a systems perspective on DASPY.

3. POSSIBLE RESEARCH THRUSTS

At a very high level I characterize the major research thrusts that are needed to make progress on DASPY as follows.

- We should continue to make progress on point solutions for various problems in data security and privacy.
- We should continue to make progress on the how aspect of application security in the narrow sense of software security.
- We should embark on research to understand the what elements of application security. There are some excellent examples of such research [1, 4, 9]. Nonetheless it needs further and explicit encouragement.
- We should embark on research to address the DASPY system challenge. Today this is largely ignored.

All four of these thrusts are deserving of support. The DASPY system challenge in particular needs special and urgent consideration. Advances in understanding the what aspects of application security are likely to be a prerequisite for progress on the DASPY system challenge.

4. CONCLUSION

The excitement generated by this inaugural conference is evidence of the growing interest in the DASPY topic, even as we develop it conceptually. I am confident this conference will contribute to advancing research in this arena.

Acknowledgment

Ravi Sandhu is partially supported by a grant from the State of Texas Emerging Technology Fund.

5. REFERENCES

[1] A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum. Privacy and contextual integrity: Framework and applications. In *IEEE Symposium on Security and Privacy*, pages 15–198. IEEE, 2006.

[2] D. Denning. *Cryptography and data security*. 1982.

[3] D. Denning and P. Denning. Data security. *ACM Computing Surveys (CSUR)*, 11(3):227–249, 1979.

[4] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebook-style social network systems. *Computer Security–ESORICS 2009*, pages 303–320, 2010.

[5] R. Gaines and N. Shapiro. Some security principles and their application to computer security. *ACM SIGOPS Operating Systems Review*, 12(3):19–28, 1978.

[6] M. Haq. Insuring individual's privacy from statistical data base users. In *Proceedings of the ACM National Computer Conference*, pages 941–946. ACM, 1975.

[7] Y. Huang, S. Huang, T. Lin, and C. Tsai. Web application security assessment by fault injection and behavior monitoring. In *Proceedings of the 12th international conference on World Wide Web*, pages 148–159. ACM, 2003.

[8] H. Katzan. *Computer data security*. Van Nostrand Reinhold, 1973.

[9] R. Krishnan, R. Sandhu, J. Niu, and W. H. Winsborough. Foundations for group-centric secure information sharing models. In *SACMAT '09: Proceedings of the 14th ACM symposium on Access control models and technologies*, pages 115–124, New York, NY, USA, 2009. ACM.

[10] B. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973.

[11] G. McGraw. Software security. *IEEE Security & Privacy*, 2(2):80–83, 2005.

[12] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation*, pages 169–178, 1978.

[13] D. Scott and R. Sharp. Abstracting application-level web security. In *Proceedings of the 11th international conference on World Wide Web*, pages 396–407. ACM, 2002.

[14] D. Scott and R. Sharp. Developing secure web applications. *IEEE Internet Computing*, 6(6):38 – 45, 2002.