Trust Research to Address Uncertainty in Security for the Smart Grid

Carl H. Hauser

***Abstract*--Perfect authentication is unachievable at the scales required for the smart grid, but we continue to design systems as if it had been achieved. Our ongoing research, using a viewpoint inspired by the concept of trust, along with results from decision theory, is attempting to provide a foundation for system design that explicitly addresses uncertainty of authentication. Although progress on the mathematical theory thus far is promising, a great deal more work is needed to understand how (or even whether) real-world behavior and experience can be modeled in the theory to make it useful in practice.**

***Index Terms*—Authentication; computer security; smart grids; uncertainty;**

I. Introduction

"Intelligent" electronic devices; "smart" meters; "flexible" AC Transmission System devices; the "smart" grid; billions of taxpayer, investor, and consumer dollars spent in hopes of achieving higher reliability, efficiency, and use of renewable energy sources in the electric power system based on computer and communication technology. An optimist sees many opportunities where smart grid technology can be beneficial. A pessimist points out that the benefits accrue only when the technology works as intended and that in the present-day cyber climate every computer-based system is eventually an attack target.

The old approach of engineering for failures arising from accident, misfortune, aging, and other more-or-less randomly governed processes is insufficient in a world where people engineer sophisticated cyber attacks aimed at particular industrial, commercial, and even security-infrastructure facilities [1] [2] [3]; and where criminal gangs co-opt personal computers by the tens of thousands to serve in their 'bot armies used to seek out and capture, for example, financial account access information from other individuals and businesses.

In the face of this evidence, conventional approaches to security: passwords and public-key systems for authentication along with identity- and role-based authorization systems cannot be said to be working very well when embedded in the current technical and social reality. Increased reliance in the smart grid on the same technologies that are failing so badly at security in their existing uses certainly gives the pessimist a good deal to worry about. Constraints on bandwidth, computational power, and availability of networked resources, accompanied by real-time performance requirements needed for many new controls to deliver their promised benefits only increase the worry.

The thesis of our work in this area is that for the smart grid to deliver on its promises we must find ways to operate and control it that recognize that authentication and authorization will be imperfectly achieved; and that even properly authenticated and authorized parties and devices may sometimes behave incorrectly or even maliciously. System design and operating practices today mainly focus on perfecting the imperfectable: the mathematics of something like PKI are so elegant and compelling that it seems like it really should be possible to *know* that the party with whom you're communicating is a particular individual. But keys are mislaid or disclosed, certificate authorities make mistakes, new entities come into existence wanting to be Certificate Authorities (CAs), and the mathematical elegance becomes overlaid with layer upon layer of revocation lists, root CA lists, on-line certificate verification services and other patches all attempting to arrange things so that when all the tests have been passed authentication is certain. Of course, it is *not* certain, but we have no choice but to pretend that it is, because our current tools for thinking about authentication would otherwise force us to *always* treat the other party as unauthenticated. And then we would be unable to ever get any work done.

II. Trust

The concept of trust provides some insights about this problem. Many different definitions of trust have been promulgated in the social sciences as well as in computer science. The one that we prefer says that trust is *reliance on*

This research was funded in part by Department of Energy Award Number DE-OE0000097 (TCIPG) and by matching funds provided by Washington State University.

C. H. Hauser is with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164 USA (e-mail: hauser@eecs.wsu.edu).

another's ability and intention to perform as expected. (Note that under this definition saying that something is *trusted* is not a positive statement -- it's a warning sign to proceed carefully!) Trusting something (or someone) is a *prediction* about its behavior: the act of trusting contains an implicit recognition that other behaviors are possible, but the trustor decides, based on what is known about the trustee(s) and the context of the decision, to take some action and acknowledges the risk in doing so.

In this short description of trust theory, we see several elements that are potentially useful in dealing with the scale of the authentication problem for power grid monitoring and control, given the unavoidable uncertainty described above. *First*, the decision of the trustor is not, principally, a decision to trust or not trust the other party (as in [4]): rather it is a decision to proceed along a particular course of action. *Second,* trust is contextual: the degree of trust (*i.e.* reliance) depends on the particular choice that is being made. *Third,* trust cannot be looked at in isolation—uncertainty about trustees' behavior is only one part of the overall uncertainty that a decision maker tries to reason about. This last point is informative because it draws attention to the field of decision theory where substantial work exists on making optimal decisions when using uncertain evidence and when the outcomes of particular decisions are themselves uncertain [5].

III. A Probabilistic Approach

In our laboratory we are working to create probabilistic mathematical models for authentication that reflect the unavoidable uncertainty described above [6]. These models will ultimately be coupled to decision models for the kinds of control decisions that smart grid technology is intended to address. For example, consider an apparent stressed-grid situation where controlled load shedding is a possible response. The evidence on which the decision must be made includes meter readings that are probabilistically authenticated and the outcome of the load shedding depends on the response of the devices that implement it which is also probabilistic.

The principal challenge here, after working out the mathematical basis of the theory, is that to be made useful it requires at least approximate knowledge of probability distributions characterizing the uncertainty of authentication. These are generally both unknown and time-varying. What sort of data gathering or analysis, if any, could provide enough information about the distributions to make the theory useful?

IV. Conclusion

We argued that today's pursuit of perfect authentication is unachievable at the scales required for the smart grid, but we continue to design systems as if it had been achieved. Ongoing research, using a viewpoint inspired by the concept of trust along with results from decision theory, is attempting to provide a foundation for system design that explicitly addresses uncertainty of authentication. Although progress on the mathematical theory thus far is promising, a great deal more work is needed to understand how (or even whether) real-world behavior and experience can be modeled in the theory to make it useful in practice.

V. References

[1] Nicolas Falliere, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier", Symantec Security Response, Version 1.4, Feb. 2011. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[2] Tom Gjelten, "Secret Cable: China Said to Coordinate Google Attack," National Public Radio, Dec. 2011. Available: http://www.npr.org/2010/12/07/131863666/secret-cable-china-said-to-coordinate-google-attack

[3] Paul Mutton, "StartSSL suspends services after security breach", Netcraft, June 2011. Available: http://news.netcraft.com/archives/2011/06/22/startssl-suspends-services-after-security-breach.html

[4] Jingwei Huang and David M. Nicol. "A Formal-Semantics-Based Calculus of Trust", *IEEE Internet Computing*, 14:5, Sept-Oct 2010, pp. 38-46. Available: http://dx.doi.org/10.1109/MIC.2010.83

[5] C.P. Robert. *The Bayesian choice: from decision-theoretic foundations to computational implementation.* Springer Verlag, 2007.

[6] Yujue Wang and Carl Hauser. "An evidence-based Bayesian trust assessment framework for critical-infrastructure decision processing". Proceedings of the Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, NH. March 2011.

VI. Biography

Carl H. Hauser is an Associate Professor of Computer Science in the School of Electrical Engineering and Computer Science (EECS) at Washington State University (WSU). His research interests include concurrent programming models and mechanisms, networking, programming language implementation, and distributed computing systems. Prior to joining WSU, he worked at Xerox Palo Alto Research Center and IBM Research for a total of over 20 years. He holds degrees in computer science from Washington State University (B.S., 1975) and Cornell University (M.S., 1977, and Ph.D., 1980).