Position Paper: Secure Time Transfer for CPS

Kyle D. Wesson, Todd E. Humphreys, and Brian L. Evans
The University of Texas at Austin

***Abstract*—To secure the future of "new clockwork," research must overcome the current vulnerabilities of cyber-physical systems to malicious timing attacks. Such attacks can take a wide range of forms—from physical to cyber to a mixture of both—and can cause a wide range of impacts—from local outages to system-wide failures. This paper presents four "needs" that, if properly addressed, will lead to a better understanding of the impact of malicious timing attacks on today's CPS and offer a secure time transfer protocol to defend future CPS from such threats.**

I. Overview

Sub-millisecond-accurate time transfer is required to ensure efficient and reliable operation in wireless telecommunications (where, for example, CDMA2000 base stations maintain 10 μs timing accuracy), smart power grids (where phasor measurement units require 26.5 μs timing accuracy), and financial trading (where high-frequency traders increasingly demand even sub-microsecond timing accuracy).

Future networks of CPS will require ever-more-accurate time synchronization for two reasons: (1) networked CPS can be made more efficient as inter-nodal synchronization improves and (2) accurate time synchronization across geographically dispersed CPS networks underpins network reliability. For sub-millisecond-accurate synchronization, there are basically two time transfer options: wireless or wireline Precision Time Protocol (PTP) implementations (or other similar protocols) for local-area networks and use of the Global Position System (GPS) for wide-area—even global—networks. Despite the critical nature of many CPS applications, the technologies typically employed to achieve sub-millisecond time transfer, including PTP/IEEE 1588 and civil GPS, lack security mechanisms, leaving them vulnerable to various timing manipulation attacks [1]–[3]. It follows that CPS reliant upon these technologies are themselves vulnerable.

Timing attacks can be broadly classified into three categories that are described next. These types of timing attacks and the associated vulnerabilities of CPS inform a list of needs for research on time-critical aspects of CPS.

A. "Physical" Timing Attacks: Civil GPS Signal Spoofing

Spoofing is the transmission of matched-GPS-signal-structure interference in an attempt to commandeer the tracking loops of a victim receiver and thereby manipulate the receiver's timing or navigation solution [4]. A spoofer can induce timing and positioning errors subtly, leaving the victim receiver unaware that its navigation solution is incorrect. Spoofing attacks have successfully attacked a wide-variety of civil GPS receivers including those employed for power monitoring [1] and in unmanned aerial vehicles [5].

B. "Cyber" Timing Attacks: Internet and Wireless Networks

Timing attacks can also leverage the cyber connectivity of CPS. Because accurate time synchronization is critical for correct network operation, cyber-based timing attacks could target many components of the network stack, causing significant problems for CPS, including:

- a failure of medium access control protocols such as [6] due to expensive packet collisions;
- reduced network performance in multihop systems due to incorrect network routing [7]; or,
- TCP timeout leading to long idle times and high congestion [8].

C. Hybrid "Cyber-Physical" Timing Attack

In addition to the strictly physical or strictly cyber attacks described above, a new type of potentially harmful attack can preys on a timing system's dual presence as an agent in both the cyber and physical domains. In this attack, a GPS receiver's software could be compromised so that a data bridge was created between the part of the receiver that handles the incoming navigation data and the receiver's network interface. Such a slight change to the receiver's software, even if detected, would appear innocuous. But when commandeered at some later time by a specially-designed GPS spoofer, the receiver would become a conduit for passing malicious programs into the CPS. The persistent availability of an unprotected conduit would allow attackers to continually adapt the malicious packages they inject into CPS network.

II. Needs to Ensure Secure Time Transfer

The vulnerabilities that can be exploited through timing attacks must be addressed to secure the future of "new clockwork." To do so requires addressing the following research needs:

Need: Quantify Impacts of Timing Attacks on In-Situ *CPS*

The response of a particular CPS will be unique unique: some attacks will cause only local effects or inconvenience a small number of users while other attacks could result in a cascade of system-wide, large-scale failures that directly impact numerous users or services. Therefore, research is needed to quantify the impacts of timing attacks on currently-fielded CPS. By quantifying the effects of attacks on various systems, a better understanding of the threat and risk models will emerge and lead to better practices for both design and implementation of future CPS.

White Paper Submitted to National Workshop on the New Clockwork for Time-Critical Cyber-Physical Systems, Baltimore, MD, October 2012

Need: Develop General Metric of CPS Dependence on Time Synchronization

Because of the wide range of applications and scenarios in which CPS can be deployed, system engineers and designers will need to determine the risks and vulnerabilities of a particular CPS or CPS-subsystem to timing attacks without necessarily carrying off actual attacks. A general metric that measures CPS dependence on time synchronization could inform their appropriate deployment. The metric would have to recognize that some CPS are uniquely vulnerable to timing manipulation because (1) their timing requirements are strict and (2) the likelihood and consequences of violating these requirements are significant. An appropriate metric will be developed only by examining a broad array of timing-dependent CPS and looking for ways to model and quantify their responses to timing attacks.

Need: Formulate Probabilistic Theory of Secure Time Transfer

Secure time transfer (STT) and message authentication, which ensures data security, can be distinguished by their security models. Message authentication is predicated on the computational infeasibility of (1) performing a brute-force search for the secret signing key or of (2) reversing one-way hash functions—tasks whose probability of success is vanishingly small [9]. In contrast, the intrinsic security of STT is weaker and demands a probabilistic security model because the information of interest in a time transfer application is conveyed through the signal timing in addition to the modulated data [10]. A probabilistic framework for STT involves a combined cryptographic and statistical approach that spans several network abstraction layers.

Need: Develop a Secure Time Transfer Protocol

To defend against timing attacks, an actual protocol for secure time transfer will need to be developed. Insofar as possible, these new protocols will be developed as extensions to existing protocols such as civil GPS and PTP and will be suited for both wireless and wireline time transfer.

III. Conclusion

Timing attacks against CPS are a serious threat to the myriad sectors they support. The study of secure time synchronization promises to be an exciting, rewarding, and worthwhile pursuit that will ensure efficient and effective CPS now and into the future. For future CPS to be efficient, reliable, and secure, there is a great need to better understand the building blocks of secure time synchronization.

Contact

Kyle Wesson (corresponding author)
The University of Texas at Austin
Electrical and Computer Engineering Department
kyle.wesson@utexas.edu

Biographies

Kyle D. Wesson is pursuing a Ph.D. in the Department of Electrical and Computer Engineering at The University of Texas at Austin where he received his M.S. He received his B.S. in Electrical and Computer Engineering from Cornell University. He is a member of the UT Radionavigation Laboratory, Embedded Signal Processing Laboratory, and the Wireless Networking and Communications Group. His research interests include GNSS security and interference mitigation.

Todd E. Humphreys is an assistant professor in the department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin and Director of the UT Radionavigation Laboratory. He received a B.S. and M.S. in Electrical and Computer Engineering from Utah State University and a Ph.D. in Aerospace Engineering from Cornell University. His research interests are in estimation and filtering, GNSS technology, GNSS-based study of the ionosphere and neutral atmosphere, and GNSS security and integrity.

Brian L. Evans is the Engineering Foundation Professor of Electrical and Computer Engineering at The University of Texas at Austin and Director of the Embedded Signal Processing Laboratory. He earned his B.S. degree from the Rose-Hulman Institute of Technology, and his M.S. and Ph.D. degrees from the Georgia Institute of Technology. Prof. Evans research bridges the gap between signal processing theory and embedded real-time implementation in the application spaces of digital communications and digital image/video processing.

References

[1] D. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[2] D. Shepard, T. Humphreys, and A. Fansler, "Evaulation of the vulnerability of Phasor Measurement Units to GPS spoofing," in *Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Washington, DC, 2012.

[3] A. Treytl and B. Hirschler, "Practical application of 1588 security," in *International IEEE Symposium on Precision Clock Synchronization for Measurement, Control, and Communication*, Ann Arbor, MI, Sept. 2008.

[4] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2008.

[5] R. N. Charette, "Commercial drones and GPS spoofers a bad mix," in *IEEE Spectrum Risk Factor*, 2012.

[6] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the mac-level behavior of wireless networks," in *Proc. of SIGCOMM*, 2006.

[7] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multihop wireless ad hoc networking routing protocols," in *Proc. of ACM MOBICOM*, 1998.

[8] J. Padhye and S. Floyd, "On inferring tcp behavior," in *Proc. of ACM SIGCOMM*, 2001.

[9] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

[10] J. Levine, "A review of time and frequency transfer methods," *Metrologia*, vol. 45, pp. S162–S174, 2008.