Balancing of Dependability and Security in Online Auctions

Lorenz Froihofer and Karl M. Goeschka
Vienna University of Technology
Institute of Information Systems
Argentinierstrasse 8/184-1
1040 Vienna, Austria
{*lorenz.froihofer|karl.goeschka*}*@tuwien.ac.at*

Abstract

Dependability and security are two system concerns that cannot be considered independently. Solving a dependability problem might introduce new challenges for security and vice versa. In this paper we contribute to this discussion with a corresponding example in the domain of online auctioning where we will show how an improvement to system dependability can introduce new security challenges.

1. Introduction

Dependability and security have been addressed traditionally by different research communities. Avižienis et al. provide "basic concepts and a taxonomy of dependable *and* secure computing" in [1]. They identify availability and integrity as two common attributes of dependability and security. Other attributes are addressed to a large extent only by one of the research communities.

While the focus of the security community lies on malicious activities and (cryptographic) countermeasures, the dependability community focuses on fault-tolerance and system robustness. However, in some cases, the effects of dependability or security violations are the same for an end-user. For example, if a service provider is not available, it makes no difference whether this is caused by a network failure, i.e., dependability concern, or a malicious distributed denial of service (DDoS) attack on the network infrastructure, i.e., security concern.

This suggests to consider countermeasures also as an integrated approach: In the case of online auctions, for example, a system can be made available during peak loads close to the deadline with resource replication. However, if we could assign a secure and tamper-proof timestamp with each bid, we could enforce the auction's deadline without requiring the timely receipt of all bids at the server. Subsequently, the peak load can be distributed along the timeline—instead of cluster load distribution. Hence, the availability could also be guaranteed through *temporal decoupling* of the communication partners. This exemplifies the key idea of our approach—to balance between dependability and security means for system availability.

2. Dependability/Security balancing

TRADE—trustworthy adaptive quality balancing through temporal decoupling—is a research project addressing high dependability and security in the domain of online auctioning of state bonds. The original motivation stems from two dependability requirements: to be able to handle high peak loads during auction deadlines and to tolerate network and server failures even during the period of an auction deadline. These two requirements are paired with the requirement for cost optimization. Differently to world-wide auctioning systems, such as eBay, that continuously run several auctions in parallel and where deadlines can be distributed to show a rather balanced system load, the considered online auctioning systems only serve a few auctions per year and consequently it is not worth to invest too much into server and network hardware.

One typical problem of auctioning systems is the fact that nearly all of the bids are delivered in the last seconds of an auction, leading to a high peak load around an auction deadline. This requires a system to be designed to handle these peak loads, while the rest of the time a high amount of system resources are unused. Additionally, network or server failures around an auction deadline may render an auction useless, requiring to repeat the auction at some time later. This may lead to financial losses as well as immeasurable losses in the reputation of the auctioneer.

These issues become less critical, if messages containing auction bids could be accepted at the server even after the

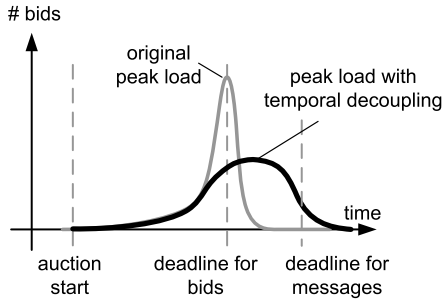

Figure 1. Effect of temporal decoupling

deadline as long as it can be guaranteed that a bid in a message was actually made before the auction deadline. More specifically, an auction bid would have to be signed with a secure and trusted timestamp in order to allow the temporal decoupling of auction bid submission and reception. Consequently, it becomes possible to resend an auction bid at some time later, if the system currently suffers from a node or link failure. Moreover, auction bids can be sent with a certain random delay after the auction deadline in order to reduce the peak load around the auction deadline.

Figure 1 illustrates this approach. In traditional online auctioning, the actions of bid submission and reception are tightly temporally coupled, i.e., the deadlines for bids and message reception are the same. This leads to the high peak load around the auction deadline. In the new temporally decoupled approach, the deadlines for submission and reception of an auction bid are different and auction bids are sent to the server with a random delay after bid submission. This leads to less load around the auction bid deadline and provides fault tolerance to the system as long as nodes or links recover from failure within the deadline for message reception. However, in case of failure it would even be possible to adaptively extend this deadline further.

While this approach improves system dependability, it introduces new security challenges. The auctioneer now has to trust the timestamps contained in the auction bids. An auction participant has the motivation to submit a bid as late as possible in order to have more time and input for decision. Consequently, s/he is tempted to fool the system by submitting the auction bid only before the message reception deadline and forge a timestamp stating the bid was sent before the bid deadline.

The approach investigated by TRADE is to provide an entity to an auction participant that synchronizes its time with the auction server and assigns correct time stamps to auction bids. However, the auctioneer cannot simply provide a piece of software to be installed at the auction participant's computer for this purpose. The auction participant may debug, reverse engineer, or otherwise tamper with the software for his/her own purposes. Consequently, we intend to integrate all the critical client-side parts of the auctioning system into a smart card that is further used for time synchronization and secure timestamping.

3. Related work

Typically, clock synchronization of computers connected via the Internet is currently performed via the Network Time Protocol (NTP) [3]. Implementations of NTP are available in all major operating systems as well as specific network devices, such as routers, for example. The roots of NTP go back to the early 1980s and since then it was continuously refined and improved, allowing for up to tens of nanoseconds in precision.

Secure digital timestamps have already been investigated to a large extent, e.g., for digital documents, and [2] discusses the main issues on their use and implementation. Generally, there are two different approaches: one that relies on a trusted third party, the secure timestamp authority (STA), to produce trusted timestamps and one that relies on the concept of distributed trust. In TRADE, a smart card should act as the STA provided by the auctioneer.

4. Conclusions

Dependability and security are two system concerns that cannot be considered independently. In this paper we contributed to the discussion of this interdependency with the problem statement and solution approach based on temporal decoupling of the research project TRADE. In the discussed scenario, dependability is enhanced by shifting parts of the solution into the security domain, thereby leveraging the interdependency between the two.

Acknowledgements This work has been partially funded by the Austrian Federal Ministry of Transport, Innovation and Technology under the FIT-IT project TRADE (Trustworthy Adaptive Quality Balancing through Temporal Decoupling, contract 816143, `http://www.dedisys.org/trade/`).

References

[1] A. Avižienis, J.-C. Laprie, B. Randell, and C. E. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Sec. Comput.*, 1(1):11–33, 2004.

[2] H. Massias, X. Serret Avila, and J.-J. Quisquater. Timestamps: main issues on their use and implementation. In *Proceedings of the IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1999. (WET ICE '99)*, pages 178–183, 1999.

[3] D. L. Mills. *Computer Network Time Synchronization: The Network Time Protocol*. CRC Press, Inc., Boca Raton, FL, USA, 2006.