SCIENCE CHINA
Information Sciences

• PERSPECTIVE •

July 2021, Vol. 64 176201:1–176201:3
https://doi.org/10.1007/s11432-020-3240-8

Privacy security in control systems

Jifeng ZHANG[1,2*], Jianwei TAN[1,2] & Jimin WANG[1,2]

[1]*Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190, *China;*
[2]*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049, *China*

Received 16 December 2020/Accepted 26 February 2021/Published online 20 April 2021

Citation Zhang J F, Tan J W, Wang J M. Privacy security in control systems. Sci China Inf Sci, 2021, 64(7): 176201, https://doi.org/10.1007/s11432-020-3240-8

Privacy issues in control systems are getting more and more attention from both industry and research. In recent years, information technology and artificial intelligence technology are being increasingly employed in emerging applications such as the Internet-of-Things [1], cloud-based control systems, smart buildings, autonomous vehicles, and 5G networks. The ubiquitous employment of such technologies provides more ways for an adversary to access sensitive information (e.g., eavesdropping on a communication channel, hacking into an information processing center, or colluding with participants in a system); therefore, the risk of privacy leakage is rapidly increasing. For example, traffic monitoring systems often collect information using position sensors from users' smartphones and release aggregated information so that users can plan their routes. However, this practice may reveal users' positional trajectories and further disclose details about their driving behavior and frequently visited locations (e.g., locations of residence and work). In addition, the consequence of privacy leakage in control systems is sometimes unbearable. In 2010, the "Stuxnex" virus invaded the Iranian nuclear enrichment infrastructure, grabbed historical running information, and conducted a replay attack to deceive the monitoring system, which further resulted in a "kill" to Iran's centrifuge and greatly postponed Iran's nuclear project [2]. Therefore, privacy security is of utmost importance for modern control systems.

What information is sensitive for a control system. A control system generally consists of a controller, a plant, and a sensor. The control inputs, states, outputs, and dynamic parameters of a system are sensitive in some application scenarios and therefore require protection from privacy attacks.

A general definition of privacy security. In order to describe the privacy issues in control systems, four subjects need to be specified firstly: the system's dynamics, the adversary's ability, the sensitive information, and the public information. The system's dynamics, which usually determines the relationship between sensitive and public information, plays a very important role in designing privacy-preserving mechanisms. The adversary's ability refers to the computing power (computationally limited or unlimited, in terms of time and storage resources) and activity type (passive adversary and active adversary). There are two types of passive adversaries: a semi-honest adversary and an eavesdropper. A semi-honest adversary refers to a system participant that follows the prescribed protocol but tries to learn the sensitive information of others, while an eavesdropper refers to an external participant who only wiretaps on communication channels. An active adversary acts arbitrarily (e.g., changing the transit information if necessary) to learn the sensitive information. The last two terms describe what information is of interest to protect and what information an adversary can learn.

Now, we try to provide a general definition of the privacy security of a system. A system is said to be privacy-secure if and only if an adversary cannot distinguish the true value of sensitive information from its candidate values given public information. A candidate value is the one corresponding to the same public information as the true value, and all candidate values of this information will be described as a candidate set below. This definition is insightful and instructive, and helps to measure privacy security. For instance, based on the number of candidate values, the dimension of the candidate set is proposed to quantify privacy security [3]. Based on the intractability of carrying out such distinguishing processes, computational security and perfect security are introduced and applied to adversaries with limited and unlimited computing power, respectively. Moreover, from the perspective of the correspondence between sensitive and public information, mutual information can be introduced to measure the privacy leakage.

How to achieve privacy security in control systems. Up to now, in the realm of control systems, some methods have been proposed to achieve privacy security. We now give a rough classification and description as follows.

• Structure technique. This technique is based on the standard observability for state reconstruction and input observability for input re-identification. The candidate sets of all possible sensitive information constitute a quotient space of the entire Euclidean space over the unobservable subspace under the standard additive operation. The bigger the dimension or cardinality of the unobservable subspace is, the

* Corresponding author (email: jif@iss.ac.cn)

more difficult it will be for an adversary to identify the true sensitive information. In other words, privacy security is achieved for a system by mapping more than one element in the sensitive information space to only one element in the public information space (i.e., the set of all possible public information). Generally, no additional effort is required to achieve privacy security if a system is unobservable. Although in many cases the system's structure is fixed, there are still some special cases in which it is possible to alter the system's structure "softly". For example, by introducing a virtual state, the algorithm proposed in [4] decomposes each agent's state into two substates and obtains a secure structure against a passive adversary.

• Deterministic transformation technique. A transformation is a mapping from the sensitive information space to another mathematical space that can be the same space of sensitive information. Privacy security is achieved by preventing the adversary from knowing the exact mapping. The candidate set of sensitive information is the preimage of all possible transformations that map to the corresponding public information. From this point of view, reconstructing the sensitive information for an adversary is not easier than identifying which transformation is used.

Frequently used methods include isomorphic (linear or affine) transformation, homomorphic encryption schemes (e.g., RSA, ElGamal, and Paillier), and time-varying transformation [5]. Although some encryption schemes like Paillier and ElGamal can transform (encrypt) one plaintext into different ciphertexts by selecting a different random parameter, the inverse transformation (decryption) maps those ciphertexts back on to the same plaintext again. So, these cryptology-based methods are essentially deterministic. Cryptology-based methods often require a large amount of computation. While other transformation-based methods have small computation loads, they are only suitable for specific systems. For practical application, homomorphic encryption schemes show great promise and have become popular in recent years, because they enable ciphertext to do certain arithmetic operations (e.g., addition or multiplication) without decryption.

Many studies have been done using this type of technique. For example, isomorphic transformation is introduced in [3] to solve the privacy issues of a cloud-based optimal control system. The Paillier encryption scheme has been used for privacy-preserving distributed optimization [6] and system identification [7].

• Stochastic obfuscation or perturbation technique. This type of method introduces randomness to systems. Viewing the relationship between sensitive and public information as a mapping, randomness can be introduced to this mapping by multiplying or adding well-designed noise to the elements of its domain or codomain. As a result, the correspondence between sensitive information and public information is no longer deterministic, even though it was one-to-one before. Therefore, the candidate set of given sensitive information corresponding to certain public information is extended and equipped with a probability distribution. Intuitively, the mutual information between the sensitive and public information is reduced, which improves the privacy security of the system. However, introducing randomness can degrade the system performance. Thus, for practical application, four key questions need to be considered when using this technique: where to introduce the perturbation, what kind of perturbation to use, how "much" privacy is needed, and what impact is brought to system performance.

Differential privacy is one of the most popular methods in this area. The privacy security degree is quantified by the privacy budget, which is an index that describes how difficult it is to distinguish adjacent sensitive information producing the same public information in a probabilistic sense. Differential privacy is conceptually simple in mathematics and resilient to post-processing, so it has been successfully applied to privacy issues for control systems, such as state estimation [8] and distributed consensus [9].

• Other techniques. Other privacy-preserving methods for control systems include secret sharing, garbled circuits, and oblivious transfer protocol. Essentially, some of these methods can be viewed as a combination of the transformation and obfuscation techniques.

In fact, each technique uses a different method to ensure the existence of the candidate set and expand the candidate set as much as possible, and therefore requires different system conditions. The structure technique and transformation technique usually have few requirements on system stability, but the stochastic obfuscation technique often requires that the system is sufficiently stable to mitigate the perturbation effect.

Challenges for privacy security in control systems. Although privacy-preserving methods, especially cryptology-based methods and differential privacy, have been proposed for traditional control systems, privacy security in control systems still faces many challenges.

• Improving efficiency for existing cryptology-based methods. Many existing studies use a partial homomorphic public-key encryption scheme to solve privacy issues in control systems, which requires a large amount of computation and is also time-consuming. Thus, optimizing the existing algorithm, designing an efficient homomorphic encryption scheme, and devising privacy-preserving outsourcing computing mechanism are eagerly desired.

• Applying more tools from cryptology to perform secure computations in control systems. Other cryptology-based methods such as fully homomorphic encryption and function encryption provide new implementation methods of secure computing. Fully homomorphic encryption supports homomorphic addition and homomorphic multiplication simultaneously. Functional encryption supports restricted secret keys that enable a key holder to learn a specific function of encrypted data but learn nothing else about the data. This kind of tool has great prospects in solving more extensive privacy issues in control systems.

• Balancing privacy security and system performance. Both quantification errors of cryptology-based methods and randomness introduced by stochastic obfuscation-based methods can degrade system performance while intensifying privacy security. However, intensifying privacy security should not sacrifice too much of the system's original performance. Therefore, additional studies regarding the relationship between these errors and system performance, especially system stability, should be conducted to design a better-performing privacy-preserving mechanism. Better privacy security metrics or perturbation methods (e.g., mini-batch method) are also needed.

• Realizing privacy security under the existence of an active adversary. Most of the existing studies investigate privacy issues assuming a passive adversary. However, an adversary can be intelligent and run any efficient strategy to achieve malicious targets while remaining undetected. How to model an active adversary's behavior and to design privacy-preserving strategies is worthy of further investigation. For example, a game theory-based method might be taken into consideration.

• Co-designing privacy-preserving algorithms, software, and hardware. The computational complexity and timeliness of privacy-preserving methods may limit their practical application. Devising specific hardware/software to efficiently realize privacy-preserving algorithms helps to extend industrial application and promotes research into privacy security. The development of application-specific integrated circuits (ASIC) and specific function libraries for privacy-preserving algorithms might be a good choice in the future.

Acknowledgements This work was supported by National Key R&D Program of China (Grant No. 2018YFA0703800) and National Natural Science Foundation of China (Grant No. 61877057).

References

1 Shen S Q, Zhang K, Zhou Y, et al. Security in edge-assisted Internet of Things: challenges and solutions. Sci China Inf Sci, 2020, 63: 220302
2 Langer R. To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve. The Langner Group, 2013. https://cyber-peace.org/wp-content/uploads/2013/06/To-kill-a-centrifuge.pdf
3 Sultangazin A, Tabuada P. Symmetries and isomorphisms for privacy in control over the cloud. IEEE Trans Autom Control, 2021, 66: 538–549
4 Wang Y Q. Privacy-preserving average consensus via state decomposition. IEEE Trans Autom Control, 2019, 64: 4711–4716
5 Altafini C. A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics. Automatica, 2020, 122: 109253
6 Lu Y, Zhu M H. Privacy preserving distributed optimization using homomorphic encryption. Automatica, 2018, 96: 314–325
7 Xu C B, Zhao Y L, Zhang J F. System identification under information security. In: Proceedings of International Federation of Automatic Control, Toulouse, 2017. 3756–3761
8 Ny J L, Pappas G J. Differentially private filtering. IEEE Trans Autom Control, 2014, 59: 341–354
9 Liu X K, Zhang J F, Wang J. Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems. Automatica, 2020, 122: 109283