COINRG
Internet-Draft
Intended status: Informational
Expires: March 12, 2021

I. Fink
K. Wehrle
RWTH Aachen University

September 8, 2020

Enhancing Security and Privacy with In-Network Computing
draft-fink-coin-sec-priv-01

Abstract

With the growing interconnection of devices, cyber-security and data protection are of increasing importance. This is especially the case regarding cyber-physical systems due to their close entanglement with the physical world. Misbehavior and information leakage can lead to financial and physical damage and endanger human lives and well-being. Thus, hard security and privacy requirements are necessary to be met. Furthermore, a thorough investigation of incidents is essential for ultimate protection. In-network computing allows the processing of traffic and data directly in the network and at line-rate. Thus, the in-network computing paradigm presents a promising solution for efficiently providing security and privacy mechanisms as well as event analysis. This document discusses select mechanisms to demonstrate how in-network computing concepts can be applied to counter existing shortcomings of cyber-security and data privacy.

Table of Contents

1. Introduction

Several deficiencies emerge from cyber-physical systems (CPS) such as the (Industrial) Internet of Things (IoT). Everyday things are equipped with sensors and CPUs to allow for automatization and make life more comfortable. The deployment of additional sensors supports the processing efficiency in Industrial Control Systems (ICS). The entanglement of the sensors with the physical world leads to high sensitivity of the transmitted and collected data. At the same time, devices are increasingly connected to the Internet to enable, e.g., processing of data on cloud servers or exchange with other systems.

Devices in CPS are often resource-constrained and do not offer the possibility to implement elaborate security mechanisms. Furthermore, legacy devices and communication protocols are often still used in industrial networks but were not designed to face the security and privacy challenges the new interconnection brings. Thus, communication and access are often unprotected, providing new attack surfaces with severe consequences: leakage of private data endangers

the users' privacy. The leakage of business secrets bears the risk of severe financial damage. Manipulation of ICSs can lead to downtimes in the best case or, financially worse, faulty production results. Last, the failure of CPS can lead to personal injury or even death. As a consequence of the described risks, we need security and privacy measures tailored to the new situation. Upgrading legacy devices with protection mechanisms is an effortful and expensive procedure. A promising approach for retrofitting security nevertheless is the deployment of suitable mechanisms within the network. To date, this is mainly realized using middle-boxes, leading to overhead and need for additional hardware.

While proper prevention and detection of attacks in the (Industrial) IoT is an unresolved issue, the after-treatment of incidents in networks offers room for general improvement. We can use network forensics to retrace and comprehend the origin and course of malicious events. However, the underlying monitoring of network traffic requires special hardware leading to high costs in traditional networks.

The common problem of all shortcomings is that traditional networking devices only allow for fixed-function deployment. Software-defined networking (SDN) enables more flexible traffic handling in the network by separating control and data plane. However, the use of fixed-function switches still restricts primary approaches like OpenFlow. Those switches match traffic against a fixed set of protocol headers to decide if and where it should be forwarded. Furthermore, consultation of the remote control plane leads to communication overhead and delays, which is especially unfavorable in the context of time-sensitive applications, e.g., in industry.

INC, in contrast, covers the shortfalls of traditional networks and SDN by allowing actual programming of the switches. This programmability leads to dynamic and custom processing of network packets at line-rate. Thus, security-related functions and packet inspection can be implemented and applied right at the switch.

This draft explores the opportunities of INC for improving security and privacy as follows: we first describe feasible mechanisms for preventing attacks and intrusion in the first place. Then, we present which mechanisms we can implement with INC for detecting intrusion and undesired behavior when it has already taken place. Last, we explore how INC can improve network forensics for analyzing and following up incidents, preventing future attacks.

2. Protection Mechanisms

The common ground for providing security and data privacy is to protect against unauthorized access. That protection is primarily provided by deploying the basic security mechanisms encryption, integrity checking, authentication, and authorization. Those are especially often missing in resource-constrained environments. [RFC7744] thoroughly discusses the need for authentication and authorization in resource-restrained environments. [RFC8576] presents security and privacy risks and challenges specific to the IoT. In the following, we describe how INC can help to retrofit suitable mechanisms.

2.1. Encryption and Integrity Checks

Encryption is critical to preserve confidentiality when transmitting data. Integrity checks prevent undetected manipulation, which can remain unnoticed even despite encryption, e.g., in case of flipped bits. Due to resource-constraints, many devices in CPS do not provide encryption or calculation of check-sums.

Complex cryptography is not supported by current programmable switches either. However, this might change in the future, which would allow retrofitting encryption and integrity checks at networking devices. Concretely, using INC with suitable hardware, data could be encrypted and supplemented with a check-sum directly at the first networking device passed by the respective data packet. The packet is then forwarded through the network or Internet to its designated destination. Decryption and integrity checks can be executed at the last networking device before the destination. Alternatively, this can be implemented at the destination if supported by the respective device. This approach does not require deployment or forwarding to additional middle-boxes. Thus, no additional attack surface or processing overhead is introduced, which is essential for time-sensitive processes as often at hand in the industry.

Overall, INC has the potential to help maintain confidentiality and integrity efficiently, and thus the availability of resource-constrained or legacy devices. Questions to clarify are if and at which costs hardware for enabling cryptographic calculations could and should be embedded in future generations of programmable networking devices.

2.2. Authorization and Authentication

Authorization and authentication mechanisms are needed to avoid unauthorized access to devices and their manipulation in the first place. With INC, networking devices can flexibly decide whether to forward packets, thus enforce authorization and authentication checks.

One possibility for authorization is to conduct a handshake between the sender and networking device before starting the communication with the industrial device. If not feasible in switch hardware, the respective calculations can be conducted in the control plane. In the case of success, the sender is added to a list of authorized communication partners. The decision is then enforced by the switch. Since authorization is only needed when starting or refreshing a connection, the necessity and overhead for consulting the control plane are limited.

The sender can append a secret token for authentication to packets directed to an industrial device. Then, the last networking device can authenticate the sender and forward the actual data only in case of success and drop it otherwise. One possibility to avoid eavesdropping of the token is the use of hash chains. Secure reinitialization can again be done using the control plane, which usually has the resources for conducting encrypted communication.

In the case of unsuccessful authorization or authentication, networking devices can inform the network administrator about possible intrusion of the system.

Undesired traffic can emerge even from authorized and authenticated devices. A solution is to add policy-based access control, on which we elaborate in the next subsection.

2.3. Behavioral and Enterprise Policies

Control processes can include communication between various parties. Even despite authorization and authentication mechanisms, undesired behavior can occur. For instance, malicious third-party software might be installed at the approved device. Regarding communication between two legacy devices, authentication might not be possible at all. An effective way to exclude malicious behavior nevertheless is policy-based access control.

[RFC8520] proposes the Manufacturer Usage Description (MUD), a standard for defining the communication behavior of IoT devices, which use specific communication patterns. The definition is primarily based on domain names, ports, and protocols (e.g., TCP and

UDP). Further characteristics as the TLS usage [I-D.draft-reddy-opsawg-mud-tls-03] or the required bandwidth of a device [I-D.draft-lear-opsawg-mud-bw-profile-01] can help to define connections more narrowly.

By defining the typical behavior, we can exclude deviating communication, including undesired behavior. Likewise to IoT devices, industrial devices usually serve a specific purpose. Thus, the application of MUD or similar policies is possible in industrial scenarios as well.

The problem that remains to date is the efficient enforcement of such policies through fine-granular and flexible traffic filtering. While middle-boxes increase costs and processing overhead, primary SDN approaches as OpenFlow allow only filtering based on match-action rules regarding fixed protocol header fields. Evaluation of traffic statistics for, e.g., limiting the bandwidth, requires consultation of the remote controller. This leads to latency overheads, which are not acceptable in time-sensitive scenarios.

In contrast, the INC paradigm allows flexible filtering even concerning the content of packets and connection metadata. Furthermore, traffic filtering can be executed at line-rate in the switch.

Going one step further, not only network communication behavior of devices can be defined in policies. As [KANG] shows, INC can be used to consider additional (contextual) parameters, e.g., the time of day or activity of other devices in the network. Furthermore, companies can define advanced policies to, e.g., authorize specific users or subnets.

While the presented policies aim to restrict communication to its designated purpose, we can use access control to explicitly address individual devices' security vulnerabilities as described next.

2.4. In-Network Vulnerability Patches

Resource-constrained devices are typically hard to update. Thus, device vulnerabilities often cannot be fixed after deployment. As a remedy and special case of policies, rules can be defined to describe known attacks' signatures. By enforcing these rules at programmable networking devices, e.g., by dropping matching traffic, INC offers an efficient way to avoid exploitation of device vulnerabilities. Further advantages are the potentially easy and extensive roll-out of such "in-network patches" in the form of (automatic) software updates of the network device.

Future research is needed to evaluate the potential and benefits of in-network patches compared to traditional security measures, e.g., firewalls, and provide proof of concepts using existing devices and vulnerabilities.

Besides presented security mechanisms, data protection mechanisms are required to preserve business secrets and the privacy of individuals. We show in the following subsection how INC can contribute to data anonymization.

2.5. Anonymization

Due to its interconnection with the physical world, the generation of sensitive data is inherent to CPS. Smart infrastructure leads to the collection of sensitive user data. In industrial networks, information about confidential processes is gathered. Such data is increasingly shared with other entities to increase production efficiency or enable automatic processing.

Despite the benefits of data exchange, manufacturers and individuals, might not want to share sensitive information. Again, deployment of privacy mechanisms is usually not possible at resource-constrained or legacy devices. INC has the potential to flexibly apply privacy mechanisms at line-rate.

Data can be pseudonymized at networking devices by, e.g., extracting and replacing specific values. Furthermore, elaborate anonymization techniques can be implemented in the network by sensibly decreasing the data accuracy. For example, concepts like k-Anonymity can be applied by aggregating the values of multiple packets before forwarding the result. Noise addition can be implemented by adding a random number to values. Similarly, the state-of-the-art technique differential privacy can be implemented by adding noise to responses to statistical requests.

Even though the INC paradigm shows the potential to deploy described privacy mechanisms within the network, research is needed to clarify the proposed concepts' feasibility.

3. Intrusion and Anomaly Detection

Ideally, attacks are prevented from the outset. However, in the case of incidents, fast detection is critical for limiting damage. Deployment of sensors, e.g., in industrial control systems, can help to monitor the system state and detect anomalies. This can be used in combination with INC to detect intrusion and to provide advanced safety measures, as described in the following.

3.1. Intrusion Detection

Data of sensors or communication behavior can be compared against expected patterns to detect intrusion. Even if intrusion prevention is deployed and connections are allowed when taken individually, subtle attacks might still be possible. For example, a series of values might be out of line if put into context even though the individual values are unobtrusive. Anomaly detection can be used to detect such abnormalities and notify the network administrator for further assessment.

While anomaly detection is usually outsourced to middle-boxes or external servers, INC provides the possibility to detect anomalies at-line rate, e.g., by maintaining statistics about traffic flows. This decreases costs and latency, which is valuable for a prompt reaction.

Besides intrusion, anomalies can also imply safety risks. In the following, we pick up the potential of INC to support safety.

3.2. Dead Man's Switch

[I-D.draft-kunze-coin-industrial-use-cases-03] addresses the potential of INC for improving industrial safety. Detection of an anomaly in the sensor data or operational flow can be used to automatically trigger an emergency shutdown of a system or single system components if the data indicates an actual hazard. Apart from that, other safety measures like warning systems or isolation of areas can be implemented. While we do not aim at replacing traditional dead man's switches, we see the potential of INC to accelerate the detection of failures. Thus, INC can valuably complement existing safety measures.

4. Incident Investigation

After detecting an incident, it is essential to conduct Network Forensics to investigate the origin and spreading of the related activity. The results of this analysis can be used to allow for consistent recovery, to adapt protection mechanisms, and prevent similar events in the future. For enabling potential investigation, traffic records are constantly collected for each flow in a network. This requires additional hardware in large networks. Furthermore, it might be preferable to exclude, e.g., specific subnets from the analysis. This is not easily possible with traditional networking devices, leading to storage and processing overhead.

With INC, flow records can be created directly at the switch when forwarding a packet. Furthermore, record generation can be done more

flexibly, e.g., by applying fine-granular traffic filtering. Also, header fields of particular interest can be efficiently extracted. Therefore, INC can considerably decrease the load and increase the efficiency of network forensics. This leads, in turn, to a better understanding of attacks and security.

5. Security Considerations

When implementing security and privacy measures in networking devices, the networking devices' security and failure resistance is critical. Related research questions to clarify in the future are stated in [I-D.draft-kutscher-coinrg-dir-01].

6. IANA Considerations

N/A

7. Conclusion

INC has the potential to improve and retrofit security and privacy, especially in concern of resource-restrained and legacy devices.

First, INC can provide intrusion prevention mechanisms like authentication and efficient enforcement of (context-based) policies. Easily deployable in-network patches of device vulnerabilities could further improve security. Encryption and integrity checks are limited by the current hardware but might be realizable in the future.

Second, INC allows examining packet contents at networking devices, which can be used to implement fast anomaly and intrusion detection in the network.

Last, INC can contribute to an efficient and targeted incident analysis.

Investigation of the feasibility of the presented mechanisms is subject to future research.

8. Informative References

[I-D.draft-kunze-coin-industrial-use-cases-03]
Kunze, I. and K. Wehrle, "Industrial Use Cases for In-Network Computing", draft-kunze-coin-industrial-use-cases-03 (work in progress), September 2020.

[I-D.draft-kutscher-coinrg-dir-01]
Kutscher, D., Karkkainen, T., and J. Ott, "Directions for Computing in the Network", draft-kutscher-coinrg-dir-01 (work in progress), November 2019.

[I-D.draft-lear-opsawg-mud-bw-profile-01]
Lear, E. and O. Friel, "Bandwidth Profiling Extensions for MUD", draft-lear-opsawg-mud-bw-profile-01 (work in progress), July 2019.

[I-D.draft-reddy-opsawg-mud-tls-03]
Reddy, T., Wing, D., and B. Anderson, "MUD (D)TLS profiles for IoT devices", draft-reddy-opsawg-mud-tls-03 (work in progress), January 2019.

[KANG] Kang, Q., Morrison, A., Tang, Y., Chen, A., and X. Luo, "Programmable In-Network Security for Context-aware BYOD Policies", In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), August 2020, <https://www.usenix.org/conference/usenixsecurity20/presentation/kang>.

[RFC7744] Seitz, L., Ed., Gerdes, S., Ed., Selander, G., Mani, M., and S. Kumar, "Use Cases for Authentication and Authorization in Constrained Environments", RFC 7744, DOI 10.17487/RFC7744, January 2016, <https://www.rfc-editor.org/info/rfc7744>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

[RFC8576] Garcia-Morchon, O., Kumar, S., and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges", RFC 8576, DOI 10.17487/RFC8576, April 2019, <https://www.rfc-editor.org/info/rfc8576>.

Authors' Addresses

Ina Berenice Fink
RWTH Aachen University
Ahornstr. 55
Aachen D-52062
Germany

Phone: +49-241-80-21419
Email: fink@comsys.rwth-aachen.de

Klaus Wehrle
RWTH Aachen University
Ahornstr. 55
Aachen D-52062
Germany

Phone: +49-241-80-21401
Email: wehrle@comsys.rwth-aachen.de