External Awards

CSS2019 Encouragement Award
Winner: Ibuki Mishina, Koki Hamada, and Dai Ikarashi, NTT Secure Platform Laboratories
Date: October 23, 2019
Organization: Information Processing Society of Japan

For "Realization of Practical Secure Deep Learning."
Published as: I. Mishina, K. Hamada, and D. Ikarashi, "Realization of Practical Secure Deep Learning," Computer Security Symposium 2019, Nagasaki, Japan, Oct. 2019 (in Japanese).

CSS2019 Encouragement Award
Winner: Koki Hamada, Dai Ikarashi, Ibuki Mishina, and Ryo Kikuchi, NTT Secure Platform Laboratories
Date: October 23, 2019
Organization: Information Processing Society of Japan

For "A Secure Batch Function Evaluation Algorithm and Its Application to Secure Logistic Regression Algorithm with High Accuracy."
Published as: K. Hamada, D. Ikarashi, I. Mishina, and R. Kikuchi, "A Secure Batch Function Evaluation Algorithm and Its Application to Secure Logistic Regression Algorithm with High Accuracy," Computer Security Symposium 2019, Nagasaki, Japan, Oct. 2019 (in Japanese).

CSS2019 Encouragement Award
Winner: Dai Ikarashi, NTT Secure Platform Laboratories
Date: October 23, 2019
Organization: Information Processing Society of Japan

For "Secure Real Number Operations for Secure AI –O(|p|)-bit Communication and O(1)-round Right Shift Protocol–."
Published as: D. Ikarashi, "Secure Real Number Operations for Secure AI –O(|p|)-bit Communication and O(1)-round Right Shift Protocol–," Computer Security Symposium 2019, Nagasaki, Japan, Oct. 2019 (in Japanese).

CSS2019 Outstanding Paper Award
Winner: Toshinori Usui, NTT Secure Platform Laboratories/Institute of Industrial Science, The University of Tokyo; Kazuki Furukawa, The University of Electro-Communications; Yuto Otsuki, Tomonori Ikuse, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, NTT Secure Platform Laboratories; Kanta Matsuura, Institute of Industrial Science, The University of Tokyo
Date: October 23, 2019
Organization: Information Processing Society of Japan

For "Automatically Appending Multi-path Execution Functionality to Vanilla Script Engines."
Published as: T. Usui, K. Furukawa, Y. Otsuki, T. Ikuse, Y. Kawakoya, M. Iwamura, J. Miyoshi, and K. Matsuura, "Automatically Appending Multi-path Execution Functionality to Vanilla Script Engines," Computer Security Symposium 2019, Nagasaki, Japan, Oct. 2019 (in Japanese).

Papers Published in Technical Journals and Conference Proceedings

Comparative Study on Layered Light-field Displays and Optimization Methods
K. Maruyama, K. Takahashi, T. Fujii, M. Date, and H. Kimata
Proc. of the International Display Workshops (IDW) 2019, pp. 1073–1076, Sapporo, Japan, November 2019.

We focus on two factors that affect the performance of layered light-field displays: the layer device and optimization method. We quantitatively compared the performances of different architectures of layered light-field displays (liquid crystal panel (LCD), holographic optical element (HOE), and super-in plane switching LCD) and their optimization methods (analytical and CNN-based methods).

Depth-range Control in Visually Equivalent Light Field 3D (VELF3D) Display
M. Date, S. Shimizu, and H. Kimata
Proc. of IDW 2019, pp. 65–68, Sapporo, Japan, November 2019.

Light field displays have limited display depth range, which is a serious issue in supporting live action content. Though generating depth maps and re-rendering is a solution, it incurs huge computational cost. In this paper, we discuss achieving depth-range compression simply by calculating the weighted average of multi-camera images.

Privacy-preserving Support-vector-machine Computing Using Random Unitary Transformation

T. Maekawa, A. Kawamura, T. Nakachi, and H. Kiya

IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E102-A, No. 12, pp. 1849–1855, December 2019.

We propose a privacy-preserving support vector machine (SVM) computing scheme is proposed. Cloud computing has been spreading in many fields. However, cloud computing has serious issues for end users, such as the unauthorized use of cloud services, data leaks, and privacy being compromised. Accordingly, we propose a privacy-preserving SVM computing scheme. We focus on protecting visual information of images by using a random unitary transformation and discuss some of the properties of the protected images. The proposed scheme enables us not only to protect images but also to experience the same performance as that of unprotected images even when using typical kernel functions such as the linear kernel, radial basis function kernel, and polynomial kernel. The scheme can also be directly carried out using well-known SVM algorithms without the need to prepare any algorithms specialized for secure SVM computing. In an experiment, we applied the proposed scheme to a face-based authentication algorithm with SVM classifiers to confirm its effectiveness.

OEM Finder: Hunting Vulnerable OEM IoT Devices at Scale

A. Nakajima

BlackHat Europe 2019, London, UK, December 2019.

Many consumer Internet of Things (IoT) vendors now use an original equipment manufacturer (OEM) production model. They purchase IoT devices from OEM suppliers then customize and sell those devices under their own brands. While this production model can reduce device manufacturing costs, it could lead to high-security risks such as when the original device is vulnerable, the OEM device (re-branded device) is also vulnerable. The survey conducted by IPVM in 2017 concluded that the vulnerability found in the Hikvision's (OEM supplier's) network camera was propagated to its various OEM devices, which are sold by over 80 vendors.

Including the above case, we found that vulnerability databases (e.g., National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE)) do not include or announce OEM devices as affected by vulnerabilities. One of the probable causes is that there is still no means to find OEM devices other than asking OEM suppliers or inspecting each device manually.

To address this supply chain risk, we developed a tool called OEM Finder, which can automatically detect OEM device candidates based on the similarity of its appearance between OEM and original devices. To achieve fast, automatic, and precise OEM device detection, we adopt an object-recognition algorithm (KAZE) with k-NN and use graph kernels.

With our tool, we found more than 180 unique vulnerable OEM device candidates from over 50,000 IoT device images, which we collected from e-commerce websites. We also analyzed the latest firmware images of some of these OEM device candidates, which are distributed by OEM vendors (not OEM suppliers), and confirmed that the devices detected with our tool are indeed OEM devices. We also found that the OEM firmware images are still vulnerable.

At the end of the talk, we will publish this tool as an online search engine. By uploading a photo of vulnerable IoT devices, this web service can list the OEM device candidates that potentially contain identical vulnerabilities. We believe that our web service will help in finding vulnerable OEM devices and mitigate security risks.
