OpenFog Security Requirements and Approaches

Bridget A. Martin
Internet of Things Group
Intel
Santa Clara, CA, U.S.A.
Bridget.martin@intel.com

Frank Michaud
Corporate Strategic Innovation Group, Cisco
Rolle, Switzerland
frmichau@cisco.com

Don Banks
Architecture and Technology Group, ARM
San Jose, CA, U.S.A.
don.banks@arm.com

Arsalan Mosenia
Dept. of Electrical Engineering
Princeton University
Princeton, NJ, U.S.A.
arsalan@princeton.edu

Riaz Zolfonoon
Emerging Technology Group
RSA
Bedford, MA, U.S.A.
rzolfonoon@rsa.com

Susanto Irwan
Sensify Security
Palo Alto, CA, U.S.A.
susanto@sensify-security.com

Sven Schrecker
IoT Security Solutions
Intel
Santa Clara, CA, U.S.A.
sven.schrecker@intel.com

John K. Zao*
Dept. of Computer Science
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.
jkzao@pet.cs.nctu.edu.tw

***Abstract*—The emerging interconnection among mobile/IoT devices, Fog Nodes and Cloud Servers is creating a multi-tier pervasive communication-computing infrastructure that will one day embody billions of devices and span across elaborate hierarchies of administration and application domains. This novel infrastructure and its operation paradigms will give rise to new security challenges as well as new service opportunities. This paper provides an overview of the security landscape of OpenFog architecture as well as a survey of the functional requirements and the technical approaches currently being discussed in the OpenFog Security Workgroup. As a report of on-going work, this paper aims at stimulating further dialogue on OpenFog Security and fostering future development of novel technologies and practices.**

Keywords—Fog Computing, Internet of Things, Trusted Computing, Communication Security, Information Security, OpenFog Architecture, Common Criteria

I. Introduction

With the deployment of Next Generation Mobile Networks (NGMNs), Internet of Things (IoTs) and Edge/Fog/Cloud Computing, the world is undergoing the largest overhaul of our information service infrastructure ever. This will drastically change the ways we live, work, move around, produce goods, provide services, interact with one another and protect our planet… Naturally, along with the foreseeable benefits come the potential problems. Information security and service trustworthiness have long been identified as the preeminent issues of our heavy dependency on the global information infrastructure. The pervasive presence of the smart devices and their physical vulnerability heighten our concerns. The increasingly devastating cyber-attacks [1,2] seem to confirm our worst nightmares. The sluggish responses of the product and service vendors towards these vulnerabilities and attacks often leave us feeling helpless.

In OpenFog Consortium [3], we firmly believe that by inserting pervasive, trusted, on-demand computing services between the information providers and consumers, we can mitigate security risks and ensure service availability and responsiveness. In this position paper, the OpenFog Security Workgroup (SWG) intended to offer an overview of the security landscape of OpenFog architecture as well as a survey of the functional requirements and the technical approaches being articulated in our workgroup. The rest of this paper is divided into five sections. Section II provides an overview of the OpenFog Architecture. Section III, IV and V then present the goals and the challenges, the functional requirements and the functional-level approach of OpenFog Security respectively. In lieu of a conclusion, Section VI offers an outlook towards future development. Readers are encouraged to refer to [4] for detail description and figures.

II. Architecture

Published in February 2017, the OpenFog Reference Architecture [4] describes "a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum". This scalable pervasive computing architecture was built upon Fog Nodes, the communication and computing entities that support hardware virtualization and trusted computing on one hand while perform secure communication and service provisioning on the other. Multiple tiers of Fog Nodes may be deployed along the communication pathways between the end devices including legacy brown-field equipment, IoT sensors/actuators, mobile devices and the cloud servers. In each tier, clusters of Fog Nodes may communicate and collaborate to disseminate information and computing services while supporting load balancing, fault tolerance and coordinated responses towards network anomalies and security attacks.

Fog Nodes deployed in the Device-Fog-Cloud Continuum may perform different tasks depending on their communication bandwidth and processing power as well as their distances (in hops or latency) from the end devices and the cloud servers. Fog Nodes connected directly to the end devices mostly work as data concentrators, compressors and pre-processors. Fog Nodes in the upper tiers are often endowed more capability and bestowed with data analytic and modeling tasks. On the other hand, reactive real-time computing and cyber-physical control often take place in the Fog Nodes close to the end devices while the data-to-knowledge conversion may be performed closer to the Cloud.

III. GOALS AND CHALLENGES

Security functions are installed in OpenFog Architecture compliant systems (a.k.a. OpenFog Systems) with the purpose of achieving two goals:

1. To enable the OpenFog System to function as a *responsive*, *available*, *survivable* and *trusted* part of the Device-Fog-Cloud Continuum;
2. To offer information security and trusted computing services through the Fog Nodes to those devices and sub-systems less endowed with capability or resources to protect themselves.

The provision of OpenFog Security is often complicated by three factors: (1) the vulnerability of OpenFog Computing as a new pervasive computing paradigm; (2) the operation of many Fog Nodes in physically exposed environments; (3) the need for interoperability between the Fog Nodes and a garden variety of IoT devices.

A. Risks of Open Environment Operation

1) Physical Exposure

Unlike the cloud servers, many Fog Nodes may be physically exposed, and thus vulnerable to physical attacks. To ensure end-to-end security, it is essential to protect Fog Nodes and their external input/outputs against hardware tampering or electromagnetic eavesdropping. The level of physical security necessary to protect a Fog Node must be determined by a physical risk assessment exercise [§V.A].

2) Open Security Boundaries

In real-world applications, Fog Nodes deployed by one service provider may serve clients from the others. These clients may have different security practices and perhaps less capability in protecting themselves. These open operating scenarios without well-defined security boundaries post some of the biggest risks to OpenFog security. How to permit these devices to share information and resources while ensuring the overall security of the OpenFog System remains a major challenge. This challenge may be tamed by enforcing security policies over the hierarchies of interoperability and service domains [§V.C.2].

3) Remote Management

Most IoT devices and Fog Nodes will be managed remotely. The remote management capability enables owners to control their devices in a cost-effective way; unfortunately, it also offers opportunities for adversaries to launch various network-based attacks, and makes the detection and mitigation of these attacks more difficult and costly. OpenFog Security and Manageability Workgroups are working together to develop a decentralized domain-based service management superstructure for providing secure remote management support.

B. Hurdles in IoT-Fog Interoperation

1) Legacy Brown-Field Devices

Brown-field applications routinely reuse existing computing and storage devices during system upgrades in order to preserve the work systems and save costs. This practice often introduces security issues since these legacy devices were not designed to respect OpenFog security requirements. Therefore, legacy devices must be properly and sufficiently reinforced before they are integrated into the OpenFog System. The best practice is to deploy hardened Fog Nodes as intermediaries between the legacy devices and the rest of an OpenFog System.

2) Heterogeneous Protocols and Operation Procedures

Heterogeneity is an innate nature of OpenFog Architecture; thus, it is essential to ensure secure end-to-end communications among OpenFog entities with different capability and functions. OpenFog intends to adopt standardized set(s) of cryptographic functions and security communication protocols according to common and/or regional practices. In order for Fog Nodes to interoperate with various legacy devices, a protocol abstraction and IP adaptation layer will be developed. Some preliminary work was mentioned in §V.B.2.

3) Resource Constraints among Devices

Devices can be unprepared or unable to adequately protect themselves. For example, many IoT devices cannot implement strong cryptographic functions and thus vulnerable to spoofing and replay attacks [5,6].How the Fog Nodes can interact with these devices without compromising end-to-end security or even better to export necessary security services to these devices remain the tantalizing challenges.

C. Protection of a New Computing Paradigm

1) Multi-tenancy

Most Fog Nodes are expected to support *multi-tenancy*, in which a single software instance may serve multiple tenants/ user groups. Multi-tenancy requires logical isolation among the runtime environments for individual instances such that each instance can perform its functions without regard to the other instances, except when data/resource sharing is needed. To accomplish this, Fog Nodes must be equipped with Trusted Computing Bases and Security Policy Enforcement Engines so that they can implement process isolation, access control, resource management and Quality of Service (QoS) requirements of tenants belonging to different organizations or application domains [§V.B.1].

2) Multi-tier IoT-Fog-Cloud Mash-up

While multi-tenancy introduces complexity within a Fog Node, the distributed multi-tier deployment of Fog Nodes throughout the Device-Fog-Cloud Continuum creates another dimension of complexity to the OpenFog System. User processes running in the trusted execution environments instantiated in the Fog Nodes can interact with one another through dynamic mesh-up relations: not only that data may go through ever more sophisticated processing as they propagate from the Devices to the Cloud through multiple tiers of Fog Nodes; they can also be shared and aggregated among the Fog Nodes within the same tier. To ensure proper data/process

management, logical domain structures must be imposed along with proper policy management [§V.C.2].

IV. Requirements

Many OpenFog applications may require the Fog Nodes to be deployed in physically exposed environments, to interoperate with less trustworthy edge nodes and devices, and to provide mission critical services under stringent operational constraints. These requirements imply that OpenFog Systems must deliver more than traditional information security; they must offer information services with the assurance of responsiveness, availability, security and trustworthiness.

A. Extrinsic vs. Intrinsic Security

The assurance of security must be specified in terms of both the *extrinsic* properties of the Fog Nodes such as their adoption of standardized cryptographic functions and security protocols as well as the *intrinsic* properties such as the assurance levels of their implementation of these functions and protocols. These *intrinsic* properties assure that a *chain of trust* is built upon the Root of Trust (RoTs) and propagated to the Trusted Computing Base (TCB) of the Fog Node. Both the extrinsic and the intrinsic properties should be prescribed in terms of the necessary protection against the potential threats towards the identified assets.

B. Protection Scope

The protection scope of an OpenFog System must enclose one or more interconnecting Fog Node(s) and all the entities within the Device-Fog-Cloud Continuum that interact directly or indirectly with these Nodes. Use scenarios may include intra and inter-Fog Node interactions as well as Node-to-Device and Node-to-Cloud interactions. Interactions between Fog Nodes and legacy devices may need to be considered in brownfield deployments.

The specification of Connectivity/Interoperability Domains (CIDs) and Service/Application Domains (SADs) [§V.C.2] may further refine the protection scope at the information transfer and service support levels.

C. Threat Models

The assets guarded by the Fog Nodes may range from information including software, data and meta-data to computing, networking and storage resources and services.

Depending on their *physical exposure* and the *openness* of their security boundaries, Fog Nodes may be exposed to different threats in physical security, communication security and computing security. Threats must be ranked according to the severity of their potential impacts under different use scenarios. Intentional or accidental damage/malfunction should also be considered.

D. Goals and Deliverables

It is the mission of OpenFog Security Workgroup to guide OpenFog system developers to deploy proper protection of their assets against the threats relevant to their applications. It is also our goal to aid the development of an OpenFog security evaluation framework. Towards these ends, the Workgroup started the work on the functional security requirements of a Fog Node by adopting the Common Criteria approach [7]. A Protection Profile (PP) of Fog Node is currently under preparation. The protection profiles of smart metering gateways [8] and mobile devices [9] were referred to as examples during this process.

The security assurance requirements of Fog Nodes will be specified after the completion of the protection profile. These requirements will then be converted into the security evaluation criteria of target products. Regional testbeds and evaluation centers can then carry out the security assurance evaluation processes.

V. Approaches

The approach to node-centric OpenFog Security consists of four distinct aspects: (1) *physical security* of the Fog Nodes, (2) *end-to-end security* within the Device-Fog-Cloud Continuum, (3) *trustworthiness of user processes* executing in the Fog Nodes and (4) *security monitoring and management* among the hardware/software entities present in this Continuum. In this section, we provide an overview of the first, second and fourth aspects of this four-prone approach. Readers are referred to the on-going work in the OpenFog Smart Objects task group for the requirements and approaches to assure trustworthiness.

A. Physical Security

The level of physical security required by a Fog Node depends on how easy outsiders may access its physical components (physical exposure) and what the consequences would be if those components are compromised (usage criticality). These physical risk assessments may call for the deployment of four types of anti-tamper mechanisms: (1) resistance, (2) evidence, (3) detection and (4) response to prevent or mitigate possible physical and/or electronic attacks against the device.

Legitimate maintenance should be allowed to be performed while the anti-tamper mechanisms in place. To allow for this, the Fog Nodes should have a special (intrinsically secure) maintenance mode that can be activated by authorized personnel to temporarily disable those mechanisms while the maintenance is in progress and then to re-enable them when the maintenance procedures are completed.

B. End-to-End Security

The provision of end-to-end security to all information, services and applications residing within a Device-Fog-Cloud Continuum is accomplished by a concerted effort of *node*, *network* and *data security* protection.

1) Node Security

The development of a secure OpenFog System should begin with a secure implementation of its Fog Nodes, which in-turn should be anchored to strong Roots-of-Trust (RoTs) implemented in secure hardware or protected by hardware supported security mechanisms. *Policy enforcement engines*

(PEnPs) should also be in place to manage information flows among user processes executed on behalf of multiple tenants. Fog Nodes equipped with Trusted Computing Bases (TCBs) [10] that can extend *chains-of-trus*t from the RoTs to the user processes are capable of instantiating Trusted Execution Environments (TEEs) through hardware virtualization and trusted boots.

Various technologies can be used to implement OpenFog compatible TCBs ranging from the use of dedicated or integrated hardware RoTs to the firmware implementation of TCBs with hardware support of memory protection and secure operating modes. Hardware trusted platform modules (TPMs) complied with TCG TPM 2.0 specification [11] are examples of hardware solutions while ARM TrustZone™ is a vendor specific firmware solution. Since integrated hardware RoTs often have limited protected storage or crypto-processing power, *virtual TPMs* may have to be employed to support potentially unlimited instantiation of TEEs [12].

2) Network Security

Both *communication security* and *information security services* are provided in OpenFog Network Security.

a) Communication Security Provision

A Fog Node should provide the communication security services in conformance to X.800 recommendation [13]:

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation of Origins and Transactions (for remote attestation)

These services should be provided among all Fog-to-Cloud and Fog-to-Fog communications with the use of standardized secure transport protocols. Fog communications shall be protected by Transport Layer Security (TLS) [14] and Datagram Transport Layer Security (DTLS) [15] protocols as these have become the de-facto standards.

A *device protocol abstraction layer* may be developed to support the across-the-board IP adaptation to the edge, and a communication proxy implementing the protocol adaptation may be deployed in front of Fog Nodes in order to implement proper confidentiality and integrity controls for wired and wireless communications from Node-to-Device communication [16].

b) Information Security Service Provision

Fog Nodes equipped with TCBs and strong security mechanisms are an ideal platform to provide information security services through network function virtualization (NFV) and software defined networking (SDN).

A number of services such as Deep Packet Inspection, Application Layer Proxy, IDS/IPS, etc., should be deployed in conformance to the interoperability and service domain specifications and operated according to the domain-based security service policies.

3) Data Security

Data, meta-data and programs exist in the Device-Fog-Cloud Continuum in one of three states: (1) *data in use*, i.e. data resident in system memory during processing; (2) *data at rest*, i.e. data resident on non-volatile storage; (3) *Data in Motion*, i.e. data exchanged over the networking infrastructure. Proper protection should be bestowed on information existing in each of these states.

a) Data in Use

Data and programs reside in the memory hierarchy during processing. Information such as keying material, proprietary personal/company data and even program codes may be considered secret and should be protected from un-authorized read or alteration. Memory management units can be used to prevent unauthorized access from address spaces occupied by other virtual machines and user processes and from physical or virtual devices. Trusted hypervisors can offer additional protection by abstracting and virtualizing the hardware platform and thus confining the execution context of individual virtual machine.

b) Data at Rest

Information residing in non-volatile storage must receive basic confidentiality and integrity protection. Three mechanisms are commonly used to protect data at rest: (1) indiscriminant full storage encryption, (2) discriminant file and database encryption, (3) mandatory and discretionary access control. Role/attribute/capability-based access control must be enforced on all data access initiated by user processes. Indiscriminant or discriminant encryption should also be used to protect information residing on non-volatile storage susceptible to physical security attacks. Security credential and access control policy management must be employed to enforce proper protection.

c) Data in Motion

Information exchanged within the Device-Fog-Cloud Continuum must be protected with network security measures [§IV.B.2]. In addition, user processes executing in trusted execution environments may choose to encrypt their data using service/process specific keys. These plus proper data storage protection may further enhance information privacy.

C. Security Monitoring and Management

New threats, vulnerabilities, even simple changes in the environment may lead to the emergence of new attack vectors. Thus, OpenFog Security Monitoring and Management (SMM) must bestow an OpenFog System with the capability to respond quickly and efficiently towards the changes in the security landscape.

Security management leverages policy to define how an OpenFog System should behave while security monitoring reports how the System is actually behaving. The security management policy delivery system should be automated in order to deliver and enforce security policies to large number of Fog Nodes in real time.

Security monitoring is implemented in order for information

to be gathered in a sufficiently trustworthy manner and forwarded to the security analytics. Enabling log and telemetry collection on the Fog Nodes is the basic requirement. Ensuring the integrity, and sometimes confidentiality and integrity of the log and telemetry events must be carefully considered. The security events should be aggregated and correlated in a Security Information and Event Management (SIEM) system or similar central or distributed correlation engine. Then, situational awareness and contextual awareness triggers notifications based on both rule-based and behavioral analytics to ensure maximum threat detection likelihood.

Security communication among the SMM services shall be isolated from the data plane and control plane communications in a specific secure domain. The SMM services shall be part of this secure domain and no unauthorized entities in the fog system shall be able to communicate within this domain.

Finally, combining the SMM capabilities enables autonomous security operations. Security events and alarms generated by manual or machine based security analytics in the monitoring system should trigger manual or automated policy updates of the affected Fog Node by the security management system for *reactive security automation*. By updating the policy on Fog Nodes that are not yet under attack, a proactive security automation system can be implemented to inhibit threats from propagating through the environment.

1) Identity and Credential Management

OpenFog Systems should manage the identities and the relations of users, end devices, Fog Nodes, Cloud Servers as well as the trusted execution environments (TEEs) and the services and applications instantiated within those entities. Following are the key characteristics of an OpenFog identity management system:

- *Entity Registration*: in order to enforce end-to-end security, it is essential to ensure the authenticity of any entity before adding them to an OpenFog System. Once an entity has been registered with an OpenFog System, it must be provide with a cryptographically strong credential. A common technique is to use public-key ciphers to certify the digital identity of the entity.
- *Proxy Services*: devices with limited resources may be incapable to perform strong authentication and access control; in those cases, these functions shall be delegated to their associated Fog Nodes as their *proxies*.
- *Secure Credential Storage*: the digital identity and credentials of a Fog Node, esp. its private keys, must be securely stored. This is particularly important when the Fog Node was deployed in a hostile environment where it may be physically tampered.
- *Intermittent Connectivity:* the identity management services such as authentication and access control must remain functional even when there is no active connection to the backend identity services. These services should be made *pervasive* through collaboration among Fog Nodes.
- *Scalability:* the identity management infrastructure must be scalable and decentralized as the OpenFog Systems may be expanded through incremental addition of Fog Nodes and end devices.

2) Domain and Policy Management

Two types of logical domains, the *Connectivity / Interoperability Domains (CID)* and the *Service / Application Domains (SAD)*, were defined in order to impose an operational superstructure upon the OpenFog Architecture. Each type of domain should be associated with a data/service abstraction layer within the architecture. Furthermore, each domain should has its own operational and security policies. These policies must be enforced by the Fog Nodes in those domains.

A CID is a coarse-grained collection of OpenFog entities within a Device-Fog-Cloud continuum that can interoperate with one another via information exchanges, program migration and reuse. CIDs should be established on the *data exchange layer* in the OpenFog Architecture with Fog Nodes being their essential entities. Interoperability and security policies should be specified and enforced within every CID.

On the other hand, a SAD is a fine-grained collection of *data/ services resources* executed within a collection of trusted execution environments (TEEs) to support a specific application. SADs should be instantiated on the *service provisioning layer* in the OpenFog Architecture. User processes in the form of containers or smart objects shall be the basic entities within SADs. Operational and trusted computing policies should be specified and enforced with every SAD.

Both CIDs and SADs can be established incrementally by the owners of OpenFog entities, data and services. These owners also have the right and the responsibility to specify the operational and security policies to be enforced in these domains. Domain hierarchies may be established to refine the scopes of policy enforcement. Bridging entities may be installed to enable inter-domain interactions. A decentralized domain membership and policy management architecture is being developed between Security and Manageability Workgroups.

VI. Outlook

OpenFog Consortium proposed a pervasive heterogeneous multi-tier communication-computing architecture to provide trusted information services on demand to a wide-range of IT/OT applications. It also offers a platform for deploying and validating new technologies throughout the Device-Fog-Cloud Continuum. In the security arena, we are cultivating the concept of Security-as-a-Service (SECaaS), which will be a Fog Node based, policy driven information security service provisioning by means of network function virtualization (NFV) to the end devices that are unable or unprepared to protect themselves. SECaaS must respect the application/service domain structures and should not interfere with the business process of the applications.

Novel technologies including *distributed persistent ledgers*, specifically the 2G/3G blockchains, and *information dispersal transfers* such as the BATS codes [17] may be employed to enhance scalability and robustness of OpenFog security.

REFERENCES

[1] The Guardian, "DDoS attack that disrupted internet was largest of its kind in history, experts say". Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[2] SecureList, "WannaCry ransomware used in widespread attacks all over the world", 5:30pm, May 12, 2017. Available at: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/.

[3] OpenFog Consortium: https://www.openfogconsortium.org/.

[4] "OpenFog Reference Architecture", OpenFog Consortium, Technical Report v.1.0, February 2017. Available at: https://www.openfogconsortium.org/ra/.

[5] A. Mosenia and N. Jha, "A Comprehensive Study of Security of Internet of Things," *IEEE Trans. Emerging Topics in Computing*, DOI:10.1109/TETC.2016.2606384, 2016.

[6] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. Jha, "Wearable Medical Sensor-Based System Design: A Survey", IEEE Trans. Multi-scale Computing Systems, DOI: 10.1109/TMSCS.2017.2675888, 2017.

[7] Common Criteria: New CC Portal: https://www.commoncriteriaportal.org.

[8] Protection Profile for the Gateway of a Smart Metering System (SMWG-PP), BSI-CC-PP-0073 v.1.3, March 31, 2014. Available at: https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf.

[9] National Information Assurance Partnership (NIAP). Protection Profile for Mobile Device Fundamentals, v.3.0, June 10, 2016. Available at: https://www.niap-ccevs.org/Profile/Info.cfm?id=381.

[10] Chen, L., Franklin, J., Regenscheid, A. "Guidelines on Hardware- Rooted Security in Mobile Devices". NIST SP-600-164 (Draft). Available at: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[11] Trusted Computing Group (TCG), Trusted Platform Module (TPM) v.2.0 specification. Available at: https://trustedcomputinggroup.org/work-groups/trusted-platform-module/.

[12] Stefan Berger, Ramón Cáceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, Leendert van Doorn. "vTPM: Virtualizing the Trusted Platform Modules." IBM Research Technical Paper, RC23879, 2006. Available at: http://domino.research.ibm.com/library/cyberdig.nsf/1e4115aea78b6e7c85256b360066f0d4/a0163fff5b1a61fe85257178004eee39?OpenDocument. [Accessed: 20-Apr-2017].

[13] X.800: Security Architecture for Open Systems Interconnection for CCITT Applications. Available at: https://www.itu.int/rec/T-REC-X.800-199103-I/en.

[14] IETF network WG. Transport Layer Security (TLS) Protocol, v.1.2, RFC5246. Available at: https://tools.ietf.org/html/rfc5246.

[15] IETF network WG. Datagram Transport Layer Security (DTLS) Protocol, v.1.2, RFC6347. Available at: https://tools.ietf.org/html/rfc6247.

[16] Hummen, Heer, and Wehrle, A Security Protocol Adaptation Layer for the IP-based Internet of Things, Available at: https://www.comsys.rwth-aachen.de/fileadmin/papers/2011/2011-hummen-smartobjects-adaptationlayer.pdf

[17] Yang, Shenghao, and Raymond W. Yeung. "Batched Sparse Codes." *IEEE Transactions on Information Theory* 60.9:5322-5346, 2014.