TapCon: Practical Third-Party Attestation for the Cloud

Yan Zhai*
University of Wisconsin Madison

Qiang Cao
Duke University

Jeffrey Chase
Duke University

Michael Swift
University of Wisconsin Madison
Why Should We Trust a Remote Service?
Why Should We Trust a Remote Service?
Why Should We Trust a Remote Service?
Why Should We Trust a Remote Service?
Why Should We Trust a Remote Service?

social trust?
Why Should We Trust a Remote Service?

Google + Social Trust?
Why Should We Trust a Remote Service?

social trust?
Why Should We Trust a Remote Service?

social trust?
Why Should We Trust a Remote Service?

social trust?
Why Should We Trust a Remote Service?

Check Code identity and Configuration?

social trust?
Cloud Enables It…
Cloud Enables It…

• **Trusted**: cloud provider has very good reputation
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
Cloud Enables It...

• **Trusted**: cloud provider has very good reputation
• **Unspoofable**: tightly controlled network
• **Knowledgeable**: aware of VM identity and configuration
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

Alice

192.168.0.1
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

Alice

(1) what’s running on 192.168.0.1?

192.168.0.1
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

Alice

(1) what’s running on 192.168.0.1?

192.168.0.1

(2) Image: Spark, Firewalls…
Cloud Enables It...

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

1. What's running on 192.168.0.1?
2. Image: Spark, Firewalls…
3. Interact if identities comply with trust policy

Alice
Cloud Enables It…

- **Trusted**: cloud provider has very good reputation
- **Unspoofable**: tightly controlled network
- **Knowledgeable**: aware of VM identity and configuration
- **Motivated**: helpful to tenants in security

This is not enough...

1. **What’s running on 192.168.0.1?**
2. **Image**: Spark, Firewalls…
3. **Interact** if identities comply with trust policy

Alice
Applications are Complicated

Alice

Analytic Application

VM1

Spark
Applications are Complicated

Alice

Analytic Application

VM1

Spark

Docker
Applications are Complicated

Analytic Application

Alice

VM1

Spark

Docker

Linux
Applications are Complicated

Alice

Analytic Application

VM1
- Spark
- Docker
- Linux

VM2
- HDFS
Applications are Complicated

Alice

Analytic Application

VM1
- Spark
- Docker
- Linux

VM2
- HDFS

?
Applications are Complicated

Alice

Analytic Application

VM Image Name: Spark

VM Image Name: HDFS
Applications are Complicated

Alice

Analytic Application

VM Image Name: Spark

VM Image Name: HDFS

Hash does not make much sense to third parties!
TapCon: Attestation Platform for Containers
TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images
TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

- Attest containers to its source manifest
TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

- Attest containers to its source manifest
- Compatible with existing applications
TapCon: Attestation Platform for Containers

An IaaS service composed by locked down VMs and authenticated storage for information about containers and images

• Attest containers to its source manifest
• Compatible with existing applications
• Rich policy for what should be trusted
Overview of TapCon
Overview of TapCon

Security Group

TapCon VM

IaaS
Overview of TapCon

Security Group

TapCon VM

Build Attested Images

IaaS
Overview of TapCon

Security Group

TapCon VM

Build Attested Images

Container Management

IaaS
Overview of TapCon

- Security Group
  - TapCon VM
- Build Attested Images
- Container Management
- Authenticated Statement Storage
- IaaS
Overview of TapCon

- Security Group
  - TapCon VM

- Build Attested Images

- Container Management

- Authorizer
  - Authenticated Statement Storage

- IaaS
Overview of TapCon

Security Group

Build Attested Images

Container Management

TapCon VM

Client

Verify Code Identity and Properties

Authenticated Statement Storage

IaaS

Authorizer
Build Attested Images
Build Attested Images
TapCon Container Manager
Question: How do we connect source to images?

TapCon Container Manager
Question: How do we connect source to images?

• Identify Repository

TapCon Container Manager
Question: How do we connect source to images?

• Identify Repository

Authenticated Repo with Build Manifest

TapCon Container Manager
Question: How do we connect source to images?

• Identify Repository
• Identify Environment

Authenticated Repo with Build Manifest

TapCon Container Manager
Question: How do we connect source to images?

- Identify Repository
- Identify Environment

Authenticated Repo with Build Manifest

TapCon Container Manager

Base Tool Image

Authenticated Image
Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements
Question: How do we connect source to images?
• Identify Repository
• Identify Environment
• Publish Statements

Authenticated Repo with Build Manifest

Authenticated Image

Base Tool Image

Publish to Statement Storage

Image ID

TapCon Container Manager

Build Attested Images
Question: How do we connect source to images?

- Identify Repository
- Identify Environment
- Publish Statements

Authenticated Repo with Build Manifest

TapCon Container Manager

Publish to Statement Storage

- Image ID
- Image Source Repo

Authenticated Repo

Base Tool Image

Attested Image
Question: How do we connect source to images?
• Identify Repository
• Identify Environment
• Publish Statements

Authenticated Repo with Build Manifest

TapCon Container Manager

Base Tool Image

Authenticated Repo

Publish to Statement Storage

• Image ID
• Image Source Repo

Container Management

Attested Image

Build Attested Images
Container Management
Container Management
TapCon Container Manager
Question: How do we attest source of a container?
Question: How do we attest source of a container?

• Restrict Images
Question: How do we attest source of a container?

- Restrict Images
Question: How do we attest source of a container?

- Restrict Images

Attested Image → Launch → Container

TapCon Container Manager
Question: How do we attest source of a container?

• Restrict Images
• Net Address as ID
Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID

Diagram:
- Attested Image
- Launch
- Container
- Assign unique network address
- TapCon Container Manager

Container Management
Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements
Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements

TapCon Container Manager

- Assign unique network address
- Publish Statements to Storage

- Image ID
Question: How do we attest source of a container?
• Restrict Images
• Net Address as ID
• Publish Statements

- Attested Image
- Launch
- Container
- Assign unique network address

TapCon Container Manager

Publish to Statement Storage
• Image ID
• Network Address
TapCon Container Manager

Attested Image → Launch → Container → Assign unique network address

Question: How do we attest source of a container?
- Restrict Images
- Net Address as ID
- Publish Statements

- Image ID
- Network Address
- Launch Parameters

Publish to Statement Storage
Question: How do we attest source of a container?

- Restrict Images
- Net Address as ID
- Publish Statements

TapCon Container Manager

Assign unique network address

Publish to Statement Storage

- Image ID
- Network Address
- Launch Parameters
- ...

Container Management
• Image ID
• Network Address
• Launch Parameters
• ...

Container Management
• Image ID
• Network Address
• Launch Parameters
• …
Image Statement:
Image ID, source repo
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it.
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it.
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it.

- Image ID
- Network Address
- Launch Parameters
- ...

**Image Statement:**
Image ID, source repo

**Endorsed Properties:**
e.g. Scanned by Anti-virus software

**Verify Code Identity and Properties**

**Policy:**
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it.
Clients may have own belief about code, or it can trust an experienced party to inspect the code and endorse it.
Verify Code Identity and Properties
Verify Code Identity and Properties
Openstack

Statement Storage

Verify Code Identity and Properties
Statement Storage

TapCon VM

Openstack

Verify Code Identity and Properties
TapCon VM

Openstack

VM Image ID: TapCon
Security Group Setting

Statement Storage

Verify Code Identity and Properties
Image ID: mysql
Image source: github.com/mysql

Statement Storage

TapCon VM

Openstack

VM Image ID: tapcon
Security Group Setting
Statement Storage

TapCon VM

Openstack

Verify Code Identity and Properties

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting
Verify Code Identity and Properties

Statement Storage

- Openstack
- TapCon VM
- MySQL

Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting
Statement Storage

Image ID: mysql
NetAddress1
launch params
...

MySQL
NetAddress1

TapCon VM

Openstack

Verify Code Identity and Properties

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting
Openstack

TapCon VM

MySQL
NetAddress1

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting

Statement Storage

Verify Code Identity and Properties
InspectorA

Statement Storage

Verify Code Identity and Properties

MySQL
NetAddress1

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting
source: github.com/mysql
endorse property: Inspected by SWAMP

MySQL
NetAddress1

Container Image ID: mysql
Container Launch Params
Container Net Address
Image ID: mysql
Image Source: github.com/mysql
VM Image ID: tapcon
Security Group Setting

Statement Storage

Verify Code Identity and Properties
Statement Storage

Verify Code Identity and Properties

MySQL
NetAddress1

Speaker: InspectorA
Source: github.com/mysql
Endorse: “Inspected by SWAMP”

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting
Statement Storage

Verify Code Identity and Properties

MySQL
NetAddress1

Speaker: InspectorA
Source: github.com/mysql
Endorse: “Inspected by SWAMP”

Container Image ID: mysql
Container Launch Params
Container Net Address

Image ID: mysql
Image Source: github.com/mysql

VM Image ID: tapcon
Security Group Setting
I trust InspectorA, what's running on NetAddress1?
I trust InspectorA, What’s running on NetAddress1?

Source: github.com/mysql
Service has property “Inspected by SWAMP”
How do we know know that:

Service at 192.168.0.1:5000
has property “Inspected by
SWAMP”
Service at 192.168.0.1:5000 has property “Inspected by SWAMP”
Service at 192.168.0.1:5000 has property “Inspected by SWAMP”
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)
Service at 192.168.0.1:5000 has property “Inspected by SWAMP”(P)

VM \text{V} \text{ owns} \ 192.168.0.1, \text{ and } \text{V} \text{ is TapCon VM}
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)

V assigns port range 5000-5100 to container C

VM V owns 192.168.0.1, and V is TapCon VM
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)

V assigns port range 5000-5100 to container C

C runs image A

VM V owns 192.168.0.1, and V is TapCon VM
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)

- V assigns port range 5000-5100 to container C
- C runs image A
- A is built from source S

VM V owns 192.168.0.1, and V is TapCon VM

Verify Code Identity and Properties
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)

V assigns port range 5000-5100 to container C

C runs image A

A is built from source S

VM V owns 192.168.0.1, and V is TapCon VM

S is endorsed with P

Verify Code Identity and Properties
Service at 192.168.0.1:5000 has property “Inspected by SWAMP” (P)

V assigns port range 5000-5100 to container C

C runs image A

A is built from source S

S is endorsed with P

VM V owns 192.168.0.1, and V is TapCon VM

Verify Code Identity and Properties
Measuring TapCon Overhead

Alice

TapCon VM

Authorizer
Measuring TapCon Overhead

Alice

MySQL Container

Boot Overhead

TapCon VM

Authorizer
Measuring TapCon Overhead

Alice

Attestation Overhead

MySQL Container

Boot Overhead

TapCon VM

Authorizer
Measuring TapCon Overhead

Alice

Regular Flow

MySQL Container

TapCon VM

Boot Overhead

Attestation Overhead

Regular Flow

Authorizer
# Performance Overhead

<table>
<thead>
<tr>
<th></th>
<th>Container Boot Time</th>
<th>First Query Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>488ms (+-40ms)</td>
<td>9.6ms (+-0.3ms)</td>
</tr>
<tr>
<td>TapCon MySQL</td>
<td>497ms (+-49ms)</td>
<td>20.6ms (+-1.2ms)</td>
</tr>
</tbody>
</table>

IaaS: Openstack kilo+ Kvm  
OS: Ubuntu 14.04  
CPU: Intel E5-2630, 16 cores  
Memory: 128GB  
Network: 2x10GbE
Conclusion
Conclusion

• Social trust is not programmable
Conclusion

• Social trust is not programmable
• TapCon provides a trusted framework that connects source to containers, which gives clients more flexibility and possibilities in validating trustworthy of remote services
Future Work and Discussion
Future Work and Discussion

• TapCon binds containers to source
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor

• IaaS provider serves a unique role
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor

• IaaS provider serves a unique role
  • Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor

• IaaS provider serves a unique role
  • Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  • Incorporate hardware trust (e.g. SGX)?
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor

• IaaS provider serves a unique role
  • Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  • Incorporate hardware trust (e.g. SGX)?

• Limitation of logic trust?
Future Work and Discussion

• TapCon binds containers to source
  • Finer grained attestation?
  • What specific source properties are useful?
  • Are they available now? e.g. IBM vulnerability advisor

• IaaS provider serves a unique role
  • Attestation is only one example. What else can IaaS help to secure trust for a tenant service?
  • Incorporate hardware trust (e.g. SGX)?

• Limitation of logic trust?

Thanks & Questions?
backup
Related Works
Related Works

• Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
- Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]
Related Works

- Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
- Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]
- Restricted Functionalities: [Miklas’09], [Roy’10]
Related Works

• Cryptography: [Gentry’09], [Dijk’10], [Parno’13]
• Information Flow Control: [Andrew’97], [Zeldovich’06], [Maxwell’07]
• Restricted Functionalities: [Miklas’09], [Roy’10]
• Attestation & Access Control: [Garfinkel’03], [Sirer’11], [Baumann’14],[Hunt’16]
Assign Network Address
Assign Network Address

• IPv4 + Ports
Assign Network Address

• IPv4 + Ports
• IPv6 (every container has an unique IP)
Assign Network Address

- IPv4 + Ports
- IPv6 (every container has an unique IP)
- Kubernetes Trireme
Code Quality & Property
Code Quality & Property

• Scanned by security tools can enhance assurance of code
Threat Model
Threat Model

- IaaS provider is trusted
Threat Model

- IaaS provider is trusted
- Service owners are careless, or even malicious
Threat Model

• IaaS provider is trusted
• Service owners are careless, or even malicious
  ✦ they may accidentally run code with known vulnerabilities
Threat Model

• IaaS provider is trusted
• Service owners are careless, or even malicious
  ✦ they may accidentally run code with known vulnerabilities
  ✦ they may change the security settings at any time
IaaS Support
IaaS Support

• A metadata service stores IaaS statement
IaaS Support

- A **metadata service** stores IaaS statement
- Attested VM
IaaS Support

- **A metadata service** stores IaaS statement
- **Attested VM**
IaaS Support

• A metadata service stores IaaS statement
• Attested VM
IaaS Support

- A **metadata service** stores IaaS statement
- Attested VM
Cloud Assisted Attestation

Alice

Cloud Provider

192.168.0.1
Cloud Assisted Attestation

Alice

(1) what’s running on 192.168.0.1?

192.168.0.1

Cloud Provider
Cloud Assisted Attestation

(1) what's running on 192.168.0.1?

(2) Image: Spark, Firewalls...

Alice

192.168.0.1

Cloud Provider
Cloud Assisted Attestation

(1) what’s running on 192.168.0.1?

(2) Image: Spark, Firewalls...

(3) interact if identities meet expectation

Cloud Provider

192.168.0.1
Cloud Assisted Attestation

(1) what's running on 192.168.0.1?

(2) Image:Spark, Firewalls...

(3) interact if identities meet expectation

This is not enough...

Alice

Cloud Provider

192.168.0.1