Fog and Security

Tao Zhang, Ph.D., IEEE Fellow
Cisco Systems
Co-Founder and Board Director, OpenFog Consortium
CIO and Board Governor, IEEE Communication Society
taxhang2@cisco.com
Key Questions

1. What are fog-specific security challenges?

2. How can we address them?

3. What new opportunities are there?
What Would Change in the Fog?

**Fog Node/System**
1. Vastly diverse capabilities
2. Many have constrained resources
3. Widely varying lifespans, with HWs that cannot be upgraded or replaced easily
4. Often not managed by experts

**Environments and Operations**
1. Geographically distributed and often remote
2. More vulnerable environments
3. Often integrated with OT systems, hence inheriting OT requirements
   - Little tolerance for downtime
4. Security of fog can rely heavily on security of its environment
5. Rapid deployments
6. Pervasive ad-hoc and transient interactions
Fog-Specific Security Challenges

1. Resource-constrained fog nodes, and “things”, need external help (services) to achieve adequate security

2. “Firewalled Castles” inadequate in many scenarios

3. “Shutdown-Cleanup-Restart” incident response no longer adequate. Need
   - Proactive, adaptive, risk-proportional responses
   - Remote online threat mitigation

4. Trustworthy ways to monitor large distributed fog systems

5. New ways to keep security up to date (or survive when security is not up to date)

6. “Behavior security” increasingly important – behave “securely” even when environment is compromised

7. Trust management for ad-hoc and transient interactions

8. New requirements for solutions:
   - Highly elastic
   - Significantly more automated
   - Cause negligible inconvenience to users
Fog Security Monitoring

How can we automatically detect if a fog system is compromised?

Trustworthy and Scalable

What compromises can or cannot be detected? how? under what conditions?
New Ways to Handle Security Compromises

If compromises occur …
- Max. response is applied, regardless of severity of the compromises
- Compromised devices/systems are shut down for inspection and restoration

Other nodes could also be brought down as a result, intentionally or unintentionally

Other Nodes take collaborative actions to enable safe operation of overall system

If compromises occur …
- Evaluate risks
- Track compromises
- Allow compromised files to run if ...
- Take protective actions
- Learn to enhance future protection
- …

*in real time*
Fog-Based Security Services

- Manage security credentials for endpoints
- Update endpoint security capabilities
- Authenticate endpoints

- Protect endpoints (offloading security processing to fog)
- Establish trusted transient relations
- Monitor/report security-related status and activities
A System Approach

Applications | Fog Platform
Fog-Based Security Services | Fog Platform
Service-Enablement Layer (V, H, I)
Networking & Communications (V, H, I)
HW | SW

Fog as an Integral Part of OT System

Developers
Thank You!