Google’s BeyondCorp
CS261 Fall 2018
Edward Oakes
Corporate Network Security

- Set of enterprise applications, employees who access them
- Applications are located on a trusted private network, connected to the internet
- **Threat model**: protect against attackers from the internet
Firewall

- Firewall blocks access to internal network based on predetermined rules
- What if employees need to access remotely?
Firewall + VPN

- Firewall blocks access to internal network based on predetermined rules
- What if employees need to access remotely?
  - Set up a shared secret while on internal network, use **VPN** to tunnel when remote

*Perimeter Model*
Perimeter Model Issues

● Firewalls are hard to set up & maintain
● Vulnerable to phishing, SQL injection, etc.
● Today’s workforce is *mobile*
  ○ Remote employee productivity is important
  ○ Surge in variety and quantity of devices
BeyondCorp (Zero-Trust)

- Assume that the internal network is **unsafe**
- Access to resources is dependent on devices, users, and credentials
  - Accessible from the internet
BeyondCorp (Zero-Trust)

- Assume that the internal network is **unsafe**
- Access to resources is dependent on devices, users, and credentials
  - Accessible from the internet
- Improved employee user experience
- Thwart internal attackers
- Fine-grained resource access control
Device Identification

- Applications are only accessible to managed devices
- Maintain a central “device database”
  - Contains hardware info, OS version, etc.
Device Identification

- Applications are only accessible to managed devices
- Maintain a central “device database”
  - Contains hardware info, OS version, etc.
- Issue unique certificates to devices in the database
  - Must be stored in an audited, secure certificate store (e.g., Trusted Platform Module)
User Identification

- Maintain a User and Group Database
  - Tightly integrated with HR system
- To authenticate user credentials and two-factor, externalized single sign-on (SSO) server
  - Generates short-lived tokens
Trust Inference

- Level of trust for a given (device, user) can vary over time
- Infer a dynamic “level of trust” using multiple data sources
  - e.g., on most recent OS patch?
Access Control Engine

- Service authorization on a per-request basis
- Validates the user, group, device certificate & details, level of trust, and location
- Can provide complete or partial access
- Configured by each application
Access Proxy

- All enterprise applications are exposed via internet-facing proxy
- Applications only accept traffic from the proxy
- Enforces encryption between client and application
Access Proxy

- All enterprise applications are exposed via internet-facing proxy
- Applications only accept traffic from the proxy
- Enforces encryption between client and application

Also provides reachability, load balancing, access control, health checks, DDoS mitigation, ...
Example: Code Review
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
Potential Attacks

- MitM device and access proxy
- MitM access proxy and application
- Non-Google device with user credentials
- Google device without user credentials
- Google device with user credentials
High-Level Security Guarantees

- Only Google-managed devices can access apps
- Only authorized employees can access apps
- Traffic is encrypted between clients and apps
- Can require devices to patch their OS periodically
Discussion

● What are the disadvantages when compared to the perimeter model?
● How difficult is it to implement this model?
● Can this be leveraged to secure outbound traffic as well (e.g., data exfiltration)?