Mobility best practice

Tiered Access at Google

Google Cloud
How can IT leaders enable the productivity of employees while also protecting and securing corporate data? IT environments today pose many challenges - more diverse fleets of devices, a shift away from 'trusted networks', broadening workforce models (including contractors and full time employees) and increasing user demands for flexibility and choice in the working environment.

Traditional security models use a binary, all-or-nothing access model where access is granted solely on the basis of machine, user, and service membership into an authentication authority, such as active directory or LDAP.

Google is taking a different approach and using tiered access as one tool to address these challenges. In contrast to traditional models, tiered access provides more granular control. The level of access given to a single user or a single device may change over time based on device measurements allowing security to set access policy that considers deviations from intended device state.

At Google, the Technical Infrastructure organization manages access for the devices used by more than 61,000 employees while protecting against sophisticated adversaries. Below we outline the model that Google has adopted and continues to evolve as it’s rolled out. The first phase of roll-out has enabled access from mobile devices, while subsequent phases will expand enrollment to cover the entire fleet of Google devices.

This paper follows [previous work](#) detailing best practices for IT Admins deploying Android.
Executive summary

Tiered access is a security model that categorizes corporate services and devices into trust tiers to determine access. First, internal services are associated with a trust tier according to the sensitivity of the data. A service can have one minimum trust tier or a more granular model of access where components and/or capabilities (e.g. read or write access) have different minimum trust tiers based on risk. Second, as resource requests are made from devices, user credentials are verified and the state of the device is queried to assess its risk profile. On successful user verification, access to services is granted only if the assessed risk profile of the device matches the required trust tier.

At Google, the implementation of tiered access goes hand in hand with a larger project called BeyondCorp which challenges the traditional security assumptions that private or ‘internal’ IP addresses represented a ‘more trusted’ device than those coming from the internet. While this project is not covered here, more information can be found in the BeyondCorp papers cited at the end.

There are three main components to a tiered access system which we will look at in turn here:

- **Client base and data sources**: what is the composition of your organization’s fleet of devices and what data do you have about them?
- **Access intelligence and gateways**: what technology can you use to evaluate a set of policies and use to make access decisions? How close to access-time can these decisions be made?
- **Services to be accessed**: what services need access controls and how will you classify the sensitivity of those services?
The benefits of tiered access

Tiered access helps organizations balance user experience and convenience with security. It enables granularly enforced access and gives a precise way of expressing risk thresholds. Users have the flexibility to use a range of devices, choose less secure configurations for their convenience (such as a longer screen unlock time or removing the PIN completely), and opt into different levels of enterprise management. A user’s level of access to enterprise services will depend on the device, its current state and configuration and their user authentication.

At Google we have a culture of innovation that requires the freedom and flexibility to connect many different devices to many different assets and services. Tiered access was implemented in order to provide an access model appropriate for this very heterogeneous environment. It helps ensure the security of corporate resources while allowing users to make informed trade-offs around access and security controls.

Other organizations facing increasing heterogeneity and complexity within their networks should consider leveraging some of the concepts of tiered access to maintain the security of their data and resources being used by client devices.
The tiered access security model

As shown in the diagram below there are three main components to a tiered access system: the client base of devices, the access intelligence and gateways, and the services to be accessed. While there are many benefits to implementing tiered access, and the security benefits are well known, implementation can be quite challenging. In the following sections, the three main components of the model are described and additional detail of the implementation is provided.
Client Base and Data Sources: a known client base with access to granular data

Before being able to measure and assess trust tiers, you need to take stock of the data that you have available about your devices. Looking at the fleet of devices that connect to enterprise services, consider the data sources for gathering device state. These sources can include security reporting systems (e.g. log reporting/aggregation systems, application scanning), operating systems patch management systems and external fleet management tooling such as asset management inventories or centralized management dashboards. Collectively, this will represent your organization’s level of control of client devices and may overall inform the levels of risk associated with each tier.

At Google, internally developed systems and tools are used to collect device data from a diverse array of devices and operating systems. A combination of management tooling, operating system agents and inherent capabilities of the systems are used to retrieve state data. All data is loaded into a centralized repository of device inventory knowledge.
Classifying devices: device attributes and device state

In associating a device to a trust tier, there are two relevant types of data: the attributes of the device and the state of the device.

First, by looking at device attributes each organization will need to define what a ‘supported’ device is in the context of your IT environment. This will define the expected baseline for a device. The basic attributes that inform this baseline are the platform operating system and device vendor as that generally implies a set of security capabilities. For instance, there are several critical security controls where mobile devices generally perform well, such as support for encryption of local data, application sandboxing and the presence of Verified Boot (on Android). Knowing the platform operating system and hardware allows you to set expectations around device state based on device capabilities. It’s within this context that organization policies can be set, such as fully trusted devices (defined below) having full disk encryption enabled and reporting into security event monitoring tooling.

Second, a recently measured device state will highlight deviations from the ideal baseline state. This ongoing measurement ensures freshness of the data used for device based access decisions. Device changes (both user intended and unintended) are expected, even in tightly managed IT environments. Device state evaluations may include whether the device has applied a recent set of critical patches, whether the device is reported as lost or stolen as well as if there has been recent suspicious activity originating from the device.
Different platforms are able to exist in different trust tiers based on the intrinsic properties of the platforms, as well as the current state of specific devices. For example, an Android device at Google may access more sensitive data in higher trust tiers if it is a "Fully Managed" device, meaning it provides full device control and access to detailed system and network logs, "Fully Managed" is allowed for devices that have strict policies enforced and have patches applied in a timely manner. A lower trust tier is made accessible to BYOD devices with a work profile.

Consideration must be given to the full life-cycle of devices within this model as well. Users and IT support staff should have a method of enrolling devices into the inventory of known and measured systems, which also provides an additional opportunity to take in metadata about the enrolled device. This can be information supporting device ownership classification (i.e. enterprise owned or BYOD), carrier information to facilitate a response to lost or stolen devices, or hardware/software information to support application of controls.

At Google, users can view and manage the access of their enrolled devices via a web based portal. The intention in the future is to use this to troubleshoot access issues, at first exposing access decision reasoning to the support function, and ultimately generating clear messaging for the user population to self-service access problems.

"In associating a device to a trust tier, there are two relevant types of data: the attributes of the device and the state of the device."
Access Intelligence and Gateways: per-request evaluation

In order to assess devices at time of access, it is necessary to have an Access Control Engine that evaluates requests on a per-request basis based on a set of rules.

An Access Control Engine within the access proxy provides service-level authorization to enterprise applications on a per-request basis. The authorization decision is based on assertions about the user, the groups to which the user belongs, the device identity, and the attributes of the device from inventory systems. This becomes now the central point of enforcement for access decisions and, as a result, becomes the place where policy can be defined and managed by security.

The Trust Inferrer queries the centralized repository and using these signals infers a trust tier. The gating mechanisms used are network switches, interactive login and web proxies (Google ‘UberProxy’, see the BeyondCorp work for more information).
Services to be Accessed: services methodically matched to tiers based on risk assessments

In addition to associating devices to tiers, services and actions (e.g. read vs write, bulk actions) must also be associated to tiers. This is a methodical exercise where for each service it will be necessary to assess the sensitivity of the service and the required trust tier in order to access it. To avoid a reintroduction of binary access, it is important that all services do not get assessed as needing the highest trust tier.

At Google a system of four tiers was created - untrusted, Basic Access, Privileged Access and Highly Privileged Access. There is no 'perfect' number of tiers but rather it is a trade-off between additional granularity for risk management and more complexity in terms of user experience. In addition to these tiers, further validation of access appropriateness is sometimes also performed by service authorization checks. This allows further granular access control to be performed with additional service-specific context.

More important than choosing the number of tiers is understanding what the minimum required trust tier is for each service and action. Each service may serve multiple tiers with different subsets of access. For example, access to view a bug in Google’s bug tracking system requires a lower level of trust than that to update one.

While the description of tiers below describes the model as intended, exceptions do exist. A documented exception process can be used to allow, but also seek resolutions of, cases where the modeled service guidelines do not fit business needs.
## Trust Tiers at Google

<table>
<thead>
<tr>
<th>Tier</th>
<th>Examples of services accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Untrusted</strong></td>
<td>• No Google data or corporate services (in general)</td>
</tr>
<tr>
<td><strong>Basic Access</strong></td>
<td>• Services with limited Confidential and Need-To-Know data exposure (e.g. campus maps and bus schedules)</td>
</tr>
<tr>
<td></td>
<td>• HR data for the requesting user</td>
</tr>
<tr>
<td><strong>Privileged Access</strong></td>
<td>• Services with Confidential but not Need-To-Know data (e.g. bug tracking)</td>
</tr>
<tr>
<td></td>
<td>• HR data with manager level access</td>
</tr>
<tr>
<td><strong>Highly Privileged Access</strong></td>
<td>• Access to all corporate services, including those that contain Confidential or Need-To-Know data.</td>
</tr>
<tr>
<td></td>
<td>* Note that further authorization checks for this class of resources occur at the service and data levels as well</td>
</tr>
</tbody>
</table>

---
The future of tiered access at Google

Tiered access at Google is still evolving. The next considerations which the team is looking at are:

- **Increasing the granularity of access decisions**: While there is logic to a fixed number of tiers in the system, there will inevitably be exceptions, use cases, and risk decisions that will drive additional tiers. In the next iteration of the tiered access model, the aim is to increase the precision of access decisions while balancing the need for users to understand security requirements.

- **Adding associated user data to assessment**: In addition to data about device attributes and the state of the device, an additional piece of information to consider is the user’s observed behavior and how that compares to normal activity as analyzed with machine learning. This would help assess how much to trust both the device and the user.

- **Driving self-selection of trust tiers**: In the interest of optimizing both security and user experience, the team is looking at is how to encourage people to voluntarily move across trust tiers in real-time, dropping tiers when access is no longer needed (e.g. to be at ‘fully trusted’ for the next two hours only).

- **Improving the service on-boarding process**: Corporate services are updated or added to Google’s corporate environment all the time. Whether it’s the newest financial tooling, an internal test version of a consumer product like Gmail, or an application to help employees find the closest Google cafe, all of these services need to be classified in terms of sensitivity and risk. To scale, service owners must be empowered to make the right tier assignments themselves, which is a process that is constantly improving.

*There are a number of teams in Google’s Technical Infrastructure org who made tiered access possible: Google Enterprise Infrastructure Protection (formerly SecOps), Google CorpEng Platforms, OpsEng, AccessSRE, Service Owners, Identity and many others.*
Related Resources

BeyondCorp. A New Approach to Enterprise Security.
http://research.google.com/pubs/pub43231.html

BeyondCorp. Design to Deployment at Google.
http://research.google.com/pubs/pub44860.html