Abstract—Mobile devices are increasingly being deployed by enterprises, governments, and the military. Protecting sensitive data that will invariably reside on them is critical. Mobile devices cannot be protected by physical security the same way as stationary systems. Therefore, they must deploy strong internal protection mechanisms for access control. Policies for access control must be driven by context and risk in the environmental in which they operate. This is inherently different from traditional policy models that focus on the multi-user access control. We propose the Risk Based Mobile Access Control (RiBMAC) policy framework for mobile device access control. It uses risk factor abstractions to break down the complexity in the specification, management and evaluation of risk based policies. Its agent-centric approach can effectively integrate a large number of onboard sensors and risk assessment components in different hardware and operational configurations. RiBMAC is a simple yet powerful policy framework that is expressive, practical and scalable. RiBMAC, in conjunction with the appropriate enforcement mechanisms, can greatly improve security for tactical mobile devices.

Key Words: mobility, security, tactical, access control.

I. INTRODUCTION

Smart phones and other mobile devices are becoming ubiquitous. Enterprise, government, and the military are increasingly interested in deploying mobile applications to enhance productivity and leverage new capabilities. This means sensitive data will invariably be placed on mobile devices (see Table 1). Security will be the limiting factor for deploying mobile devices in many scenarios where they would otherwise be extremely useful. There are major management and security gaps that must be overcome before mobile devices can evolve from being consumer devices to full-fledged productivity and critical application platforms.

Table 1. Potential sensitive data on mobile devices

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Mobile banking application, internal corporate email, intellectual property</td>
</tr>
<tr>
<td></td>
<td>Customer records (e.g., medical records)</td>
</tr>
<tr>
<td>Government</td>
<td>Sensitive records (e.g., police files)</td>
</tr>
<tr>
<td>Military</td>
<td>Sensitive intelligence data, situation awareness (e.g., troop locations),</td>
</tr>
<tr>
<td></td>
<td>secret communications (voice and text), sensitive technology (e.g., software)</td>
</tr>
</tbody>
</table>

Mobile operating systems are built from the ground up with sandboxing to support secure web browsing and non-interference between applications. However, this is not enough in the context of enterprise, government, and military applications. Exploits are already happening [1,2,3,4] and the threat will only increase as more valuable data are stored on mobile devices. The current trend is to improve security by deploying standard computer security mechanisms [5,6]. They include antivirus scanners, firewalls, anti-spam software, secured networking, and encrypted storage. These measures mainly deal with network and malware threats. While it is critical to address these threats, mobility also creates new threats and vulnerabilities that must be addressed by new security mechanisms.

Security requirements for mobile devices are inherently different from stationary machines. Stationary machines operate in secure physical environments. The level of physical security typically corresponds with the sensitivity of the data and the threat level of the environment. If physical security is removed, most systems are very vulnerable. If attackers are able to gain physical access to systems, they will most likely be able to gain access to data stored inside.

Mobile devices are designed to be used on the move. They are exposed to a range of different threat environments and cannot rely on physical security. They can be used in an office, on a crowded train, inside a secured base, or on the battlefield. Mobile devices can be
easily lost or captured by the enemy (along with their users). It is also likely that mobile devices are captured in an active and unlocked state.

Depending on the sensitivity of the data and the usage scenarios, this could be a minor or an extremely serious threat. There is a tradeoff between security, functionality, and complexity of the system. In the civilian world, the value of the data and the technical proficiency of the attackers are both limited. Devices are more often lost to common thieves that are more interested in the value of the hardware. Enterprise applications that deal with corporate communications, client records, and intellectual property are indeed sensitive, but rarely critical. Furthermore, legal and law enforcement recourses are usually available that can mitigate the consequence of data loss. Availability is often more important of a concern to enterprise IT managers.

For the military, tactical mobile devices are used in the battlefield and directly in harm’s way. Common military applications such as mapping, situation awareness, intelligence, and communications all deal with extremely sensitive and highly relevant data. For example, situation awareness applications can reveal the location of other soldiers. This information can directly put lives in danger. Intelligence and planning information can put entire operations at risk. Some applications themselves could represent advanced and highly sensitive technology. Access to sensitive data must be guarded very carefully. At the same time, soldiers rely on information for advantage in the network-centric battlefield. Availability of information and applications is also critical. Therefore, robust enforcement mechanisms and sophisticated access control policies are both needed for mobile devices.

Data protection mechanisms on mobile devices need to be strong enough to withstand physical attacks from motivated and technically sophisticated attackers. Sensitive applications and data should be securely locked unless they are being actively used. Access to resources should be granted only if there is a low risk that the device is stolen or captured. The access control policy should be driven by context and risk in the environment where the mobile device is used. This is inherently different from traditional access control models that address multi-user security. The approach should be one of risk management and mitigation. Mobile devices are uniquely suited to perform risk-based access control. They have a large number of onboard sensors including radio receivers, camera, microphone, GPS, accelerometer, thermometer and barometer that could be leveraged to assess the risk in the environment. Supporting a sophisticated and fine-grained risk-based access control policy model can make up for the lack of physical security for mobile devices.

Existing security mechanisms on COTS mobile devices that address device loss provide a level of protection suitable for most consumer and civilian enterprises. Password based screen lock is the primary protection mechanism. It does not involve access control policies. Successful authentication grants access to everything on the device. More advanced security mechanisms including remote wipe and device encryption also lacks support for policies. Remote wipe is usually user initiated through the network. Device level encryption does not provide any granularity. Once decrypted, everything on the device is exposed. On the other hand, locking the device renders it completely inoperable.

This paper focuses on the risk based access control policy model for mobile devices. The policy enforcement mechanisms are discussed in other works [7]. The policy and enforcement components can be developed independently. The enforcement mechanisms need to operate on COTS mobile devices. Different enforcement mechanisms can be deployed depending on the security and operational requirement of the mobile device.

The rest of this paper is organized as follows. Section 2 discusses risk adaptive access control in the mobile device context. Section 3 discusses the need for abstraction and the RiBMAC policy framework. Section 4 offers discussion and a conclusion.

II. RISK AND CONTEXT BASED ACCESS CONTROL

Risk Adaptive Access Control (RAdAC) [7,8] is an access control model that takes into account risk and context in making access decisions. However, the existing RAdAC model and systems are not suitable in the mobile device context. We will highlight these shortcomings and outline the requirements for mobile devices in the following subsections.

A. Single User Access Control

Traditional access control models (including ACL, RBAC [9,10], ABAC [12] and RAdAC) are intended to address multi-user systems. Policies embody a mapping of permissions from subjects to objects. Identity is the most important and often the only input in access control decisions. RAdAC supports more dynamic policies that can further restrict or relax access control rules depending on the current risk and the operational need. RAdAC is revolutionary in taking into account more inputs. However, the primary focus of the RAdAC policy is still the mapping between users and resources.

Mobile devices, on the other hand, usually have a single user. Under optimal conditions, that user should have full access to all the resources on the device. Access control decisions therefore deal mostly with the context. Instead of being risk adaptive, single-user access control for mobile devices is completely risk based.

In traditional multi-user systems, authentication and authorization take place separately. Identity is an all-or-none value. The user first obtains an identity through the authentication process. Then the authorization process takes that identity as input and produces privileges
according to the policy. In single-user access control, authentication will simply serve as one of the many inputs for risk assessment and authorization. Identity is viewed as a fuzzy value derived from the strength of the authentication completed.

Single-user access control governs access to local resources on mobile devices. Traditional multi-user access control still applies when the user accesses network resources through mobile devices (figure 1).

![Network Resources](image1)

**Figure 1. Single and multi-user access controls in mobile devices**

Tactical mobile devices in the military often operate on disadvantaged or peer-to-peer networks. The thin-client approach is impractical in this context since large amounts of data is stored and processed on mobile devices. Therefore, single-user risk and context based access control is unavoidable on the mobile device layer.

B. **Multi-dimensional Risk Metric**

The current RAdAC model takes into account a large variety of inputs to assess risk. However, all the inputs are combined into a single monolithic risk metric. That value is compared against a monolithic operational-need metric to make access control decisions.

Environmental risk factors are disparate and often incompatible. Combining them to calculate a single risk metric may not produce a value that makes sense for all operational environments and resources being protected. Different applications and data are sensitive for different reasons and need to be protected differently. For example, tactical situation awareness applications that show locations of soldiers can put lives in danger. Tactical information also has a strong need-to-share even with coalition forces. However, the relevance of the data is short lived because troop positions change frequently. The primary threat is the mobile device falling into enemy hands during the battle. Intelligence applications, on the other hand, can reveal sources and methods that are long lasting. Compromise of that information can set back entire operations. The primary threat is release of information to un-cleared personnel regardless of the timeframe. Policies for these two types of information will most likely weigh risk factors very differently and use with completely different risk metrics. The risk profile for mobile devices should be detailed enough so that different applications can specify different risk metrics.

C. **Successful Implementation**

RAdAC policies and systems are inherently complex. Quantifying the risk and operational-need metrics from such a large number of disparate and interacting inputs is not trivial. Current approaches to deal with that complexity usually involve heuristics and machine learning [12]. However, complexity is not decreased using these approaches. Instead, they simply produce equally complex policy specifications that are extremely difficult to understand, validate, and enforce. There are few successful and practical implementations of RAdAC.

Applying the same approach for mobile devices is even more difficult. Mobile devices are resource constrained and will have difficulty processing complex policy decisions. Many applications on military tactical mobile devices will be extremely mission critical. Therefore, access control policies need to be crafted very carefully to achieve the correct balance between confidentiality and availability. Complex policies written by machine learning that are hard to understand and impossible to validate cannot be deployed. Furthermore, mobile devices come in a wide range of different platforms (e.g., Androids, iPhones, and Blackberry) and configurations (different onboard sensors, hardware components, and applications). This variability makes specification and management of generated policies even more difficult.

D. **Other Related Work**

There are several access control policy frameworks that take into account risk and context. Context awareness is important in pervasive computing and service oriented architecture [11,12,13]. Their focus remains on multi-user access control. Location and spatiotemporal-based access control has been proposed for mobile computing [14,15]; however, they only address location and time and do not support general risk assessment.

III. **ACCESS CONTROL MODEL FOR MOBILE DEVICES**

We propose a new risk and context based access control model for mobile devices called Risk Based Mobile Access Control (RiBMAC). It will use abstractions to reduce the complexity in the specification, management and evaluation of access control policies.

A. **Abstraction Approach**

In the beginning, access control policies are simply expressed as access control lists (ACL). Privileges are directly mapped between subjects and objects. Managing the policy as users and resources are added and removed is time consuming and error prone. As the number of users (subjects) and resources (objects) increases, this approach becomes unwieldy and impractical.

More advanced access control models such as role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control (PBAC) reduce the complexity by providing a layer of abstraction between subjects and objects. Policies can be written using these concepts as a middle layer. In RBAC for example, users are grouped into roles. Resources in turn
specify their access policies with respect to roles. There are no longer direct links between subjects and objects. When users change their roles, it automatically affects their privileges to all the resources. When access policies for resources change with respect to roles, all users are automatically affected.

Advanced access control models are successful because they reduce the complexity of the policy. In traditional multi-user access control systems, complexity arises from the large number of subjects and objects. Access control in mobile devices is single-user. Complexity arises from the large number of inputs involved in determining the current risk. Our approach in RiBMAC is to create abstractions to simplify risk-based policies in a similar way. We can do this by limiting the scope of the policy framework to tactical mobile devices. Appropriate abstraction concepts can then be developed to capture the relevant risk profile.

Instead of a single monolithic metric, risk is broken down into meaningful independent risk factor abstractions (figure 2). This approach simplifies calculation of risk because the abstractions are conceptually simpler. It is much easier to determine the proper effects of risk assessment inputs on individual risk factors. Risk factors can be broken down further into sub-factors.

A meta-policy will define the meaning of the risk factor abstractions and values. The meta-policy is defined for the entire system in the deployment scenario. Instead of producing raw inputs, risk assessment components will perform post-processing using the meta-policy to create statements that express threats and state information in terms of risk factor abstractions (figure 3). The access control policies for resources will specify the risk profile that must be satisfied to grant access written using the same meta-policy (figure 5).

The meta-policy will also specify the aggregation and de-conflict functions for risk factors. For example, two authentication components will produce two statements for the authentication risk factor. The meta-policy will define how those two statements are combined and normalized to produce a single value for the overall authentication.

B. Risk Factors for Mobile Device Policy

This section presents typical risk factor abstractions for mobile device access control in a typical operational scenario. They can be changed or further broken down for specific deployment scenarios. This involves changing the meta-policy. Access control policies for resources can use the identifier field to refer to specific inputs. For example, an application may be paired with a specific password. However, most access control policies would omit the identifier and deal with the overall risk factor value. The standard data fields that make up a risk factor statement are shown in italic.

1) Location. The location risk factor deals with specific places using the identifier. It can be broken down into five subcategories: GPS, network, peer, point, and zone. GPS coordinates indicate an absolute location. Policies can specify a distance from a specific coordinate. The other subcategories represent relative locations. Networks and peers represent entities in range of the radio receiver. Policies can require that mobile device be connected or be within close proximity to a specific network or peer nodes. Points and zones represent more abstract constructs that are derived from other location related inputs. A point is a named location while zones are named regions. For example, green-zone versus red-zone can be based on GPS coordinates, networks in range, or beacons on the perimeter. That information is processed by the risk assessment components and the mobile access control policies can simply specify green-zone without worrying about how that state is derived.

Location_GPS: (longitude, latitude, valid)
Location_Network: (ID, type, distance, status)
Location_Peer: (ID, type, distance, status)
Location_Point (ID, distance, status)
Location_Zone: (ID, status)

2) Authentication. Authentication risk factor indicates what type of authentication the user has performed. It represents a level of certainty with regard to the identity of the user. The ID field allows policies to specify a specific authentication method. The type field indicates whether the authentication is based on what you know, what you have, or what you are. Access control policies can use the type field to specify a requirement for multifactor authentication. The value field indicates the strength of the authentication. A value of 0 indicates that authentication failed. A non-zero value indicates successful authentication and represents the strength of the authentication mechanism. Individual authentication statements (e.g., successful certificate authentication, unsuccessful password authentication) are aggregated
according to the meta-policy to produce an aggregated authentication value. Policies can refer to specific authentication mechanisms using the identifier, or the overall authentication value by omitting the identifier.

**Auth:** (ID, type, value, timestamp, expiration)

3) **Timeouts.** Timeout risk factor records the events that trigger timeout in the state. The target field indicates the application in which the event occurred. The type field indicates the type of event: for example, keystroke, screen touch, movement, or voice recognition. Policies can specify timeouts for specific applications, or globally in which case all targets are considered.

**Timeout:** (target, type, timestamp)

4) **Threats.** Threat risk factor indicates danger detected in the immediate proximity of the mobile device. The value indicates the severity of the threat. Inputs are usually supplied by onboard sensors on the mobile device. For example, a component can use the microphone to detect friendly and enemy gunfire. Several peer devices can work together to triangulate the source of the gun shots and adjust the value depending on the distance from the user. The meaning of the value field and the aggregation function is agreed upon in the meta-policy. Policies can specify a specific threat using the identifier, or the overall threat value.

**Threat:** (ID, value, timestamp, expiration)

5) **Conditions.** Condition risk factor refers to the overall security posture of the operational environment. They are usually based on inputs from components outside the device and represent general alert level. For example, conditions can include terror alert levels and forced protection levels. Conditions are usually related to locations. For example, combat condition will usually go along with being in the red zone.

**Condition:** (ID, value, timestamp, expiration)

C. System Design

The policy decision engine keeps track of the current risk state. The state is simply a list of risk factor abstraction statements from risk assessment components.

```plaintext
Location_Zone(Red_Zone, active);
Location_Peer(Smith, John, Lieutenant, 45m, active);
Location_Peer(Owen, Chad, Private, 85m, detected);
Auth(PIN, know, 6, 13:45:12, 14:34:12);
Auth(Voice_Rec, 4, 13:38:23, 14:43:23);
Threat(Gun_Shot, 7, 13:38:23, 14:43:23);
Condition(Force_Protection, 5, active);
```

Figure 3. Example risk state composed of risk factor statements

Risk assessment components convert environmental, system and user inputs into abstracted risk factor statements before sending them to the policy decision engine. Most of the intelligence and complexity in the system will reside in the risk assessment components. This agent-based approach offers flexibility and supports plug-and-play for new components and configurations. Components can be developed by different vendors independently and integrated in the overall framework. Risk assessment agents will continuously produce risk factor statements to update the state. New statements will replace existing statements with the same identifier.

```
AND{
  Auth(value>7),
  Threat(value<7),
  Threat(ID=Gun_Shot, value=0),
  OR{
    Location_Zone(ID=green_zone, status=active),
    Location_Network(ID=base, status=active),
  },
  NOT{Location_Peer(status=captured, distance<50m)}
}
```

Figure 5. Example access control policy
Access control policies are specified per resource and stored in the policy enforcement point. They are included as part of the access request to the policy decision engine. The operational need metric is embodied by the different access control policies for different resources. Mission critical applications can specify less stringent access control policies. Applications with similar risk and operational need profiles can be assigned into policy groups that share the same policies to simplify system management.

The protection mechanism is also implemented on the policy enforcement point. The resource must be securely locked until access is granted. The specific mechanism depends on the security requirement of the deployment scenario.

IV. CONCLUSION

In this paper, we present the RiBMAC policy framework. It is inherently different from traditional access control frameworks and focuses on risk based access control policies for mobile devices. RiBMAC along with appropriate enforcement and protection mechanisms can make up for the lack of physical security in mobile devices.

RiBMAC uses risk factor abstractions to breakdown the complexity in the specification, management and evaluation of risk based policies. Access control policies can be written using risk factor abstractions instead of raw inputs. Intelligence and complexity in the system is pushed out of the actual policy decision engine. Individual risk assessment agents produce output in terms of shared risk factor abstractions. This agent-centric approach can effectively integrate different onboard sensors, network components, algorithms, and vendors. The same policies can be applied to mobile devices with different hardware and operational configurations. The RiBMAC policy framework is simple yet expressive, scalable, and powerful. It provides a practical approach to address pressing security issues in mobile devices.

The RiBMAC approach can also be applied to other contexts outside of mobile devices. We believe this approach can be used to successfully implement RAdeAC.

REFERENCES