Appendix A

Fabrikam Phone 1.0

The Fabrikam Phone 1.0 sample threat model is intended to present threat modeling concepts without being tied to any particular software or type of application. Fabrikam, Inc. created Phone 1.0 as its first telephone suitable for business applications. This phone has features common to consumer telephones, such as caller ID, speed dial, and an answering machine. In addition, Phone 1.0 includes an access control feature that regulates which users can make calls from the phone and access its administrative features.

Table A-1 contains the high-level information about the threat model being developed for the Fabrikam Phone 1.0. This basic information includes the type of product and its location, the owner of the threat model and its team members, and any available milestone information.

Table A-1 Threat Model Information

Product	Fabrikam Phone 1.0
Milestone	RTM
Owner	Kim Abercrombie
Participants	Alice Ciccu, Scott Gode
Reviewer	John Arthur
Location	Database\Fabrikam Phone 1.0 (Phone 1.0)
Description	The Fabrikam Phone 1.0 (Phone 1.0) is Fabrikam, Inc.'s first high-tech telephone device. The phone includes popular features such as caller ID, speed dial, and an answering machine. In addition, it has features that enable its use in semi-private areas, such as conference rooms.

Use Scenarios

Table A-2 lists the known use scenarios for the application—in other words, the expected use of Phone 1.0. Using or deploying the application in a way that violates its use scenarios could impact its security.

Table A-2 Use Scenarios

ID	Description
1	The Fabrikam Phone 1.0 application will be connected to the Public Switched Telephone Network (PSTN). The security of this network is beyond the control of Phone 1.0.
2	If Phone 1.0 is installed in a location that untrusted users can access, the application should have local access control enabled.
3	Fabrikam did not design Phone 1.0 to withstand attacks against the physical device.

External Dependencies

Table A-3 lists the external dependencies Phone 1.0 has on other components or products, which can impact security. Such external dependencies are assumptions made about the usage or behavior of these other components or products. Inconsistencies in these assumptions can lead to security weaknesses.

Table A-3 External Dependencies

ID	Description
1	Fabrikam Phone 1.0 depends on the PSTN for providing power. A two-day power cell in Phone 1.0 provides backup power should the power provided by the PSTN go down.

Implementation Assumptions

Table A-4 lists the implementation assumptions of Phone 1.0 and describes each assumption about the internal workings of the application that is made during the specification phase, but before implementation has started. These assumptions should not be violated. Typically, they will be reviewed by the threat model team further once implementation takes place.

Table A-4 Implementation Assumptions

ID	Description
1	The voice-command dialing option has yet to be implemented. If added, this option should not introduce a way for adversaries to bypass current security features, such as long-distance call lockout.
2	If encrypted communication is added to the application, key exchange should be done according to industry-accepted standards.

External Security Notes

Table A-5 lists the external security notes, which are threats or other information that an application user should be aware of to prevent possible vulnerabilities. These notes might include features that, if used incorrectly, could cause security problems for application users.

Table A-5 External Security Notes

ID	Description
1	Phone 1.0 has a remote administration interface with a default numeric password. Although the interface is disabled by default, the user should ensure that the password is changed if it the feature is enabled.
2	If the user wants to protect the speed-dial list and protect whether remote administration is enabled, he should enable local access control.
3	The long-distance password can be enabled only when local access control is enabled. Furthermore, entering the long-distance password with the keypad allows local calls to be made.
4	If the user wants to control who can make outgoing calls, local access control should be enabled.

Internal Security Notes

Table A-6 list the internal security notes, which contain security information relevant only to someone reading the threat model. These notes can be used to explain implementation choices and design decisions made due to nonsecurity factors (for example, backward compatibility or overriding business needs) that affect the system's security.

Table A-6 Internal Security Notes

ID	Description
1	Speed-dial information, voice mail messages, and the outgoing greetings are all stored in volatile RAM. Manufacturing the combination of volatile RAM and a battery backup for Phone 1.0 is cheaper than using nonvolatile RAM. However, power loss to Phone 1.0 can cause the loss of information if the battery backup is depleted.

Trust Levels

Table A-7 lists the trust levels and describes privilege levels that are associated with entry points and protected resources.

Table A-7 Trust Levels

ID	Name	Description
1	Administrator	The Phone 1.0 administrator has access to all features and can bypass all security checks.
2	Long-distance user	Phone 1.0 can be configured to restrict long-distance calling. The long-distance user is a phone user permitted to make long-distance calls.
3	Local call user	The local call user can place only outgoing local calls.
4	Denied user	Phone 1.0 can be configured to prevent access to the phone without a password. The denied user is a user with no access.
5	Anonymous remote user	The anonymous remote user represents any data or incoming calls over the PSTN.

Entry Points

Table A-8 list the entry points and describes the interfaces through which external entities can interact with the application, either directly or by indirectly supplying it with data.

Table A-8 Entry Points

ID	Name	Description	Trust Level
1	Handset	Used by the user for voice communication. Voice-activated dialing will also be implemented via this interface.	(1) Administrator (2) Long-distance user (3) Local call user (4) Denied user
2	Keypad	Used for dialing, entering local access passwords, and other administrative functions on Phone 1.0.	(1) Administrator (2) Long-distance user (3) Local call user (4) Denied user
3	Telephone line	Phone 1.0 interfaces with the PSTN via the telephone line.	(5) Anonymous remote user

Table A-8 Entry Points

ID	Name	Description	Trust Level
4	Alpha-numeric display	Shows information such as speed-dial numbers, caller ID, and administrative menus.	(1) Administrator (2) Long-distance user (3) Local call user (4) Denied user
5	Audible ringer	This is an exit point that alerts the user of incoming calls.	(1) Administrator (2) Long-distance user (3) Local call user (4) Denied user
6	Remote administration	This menu-driven interface is accessed remotely over the PSTN. The interface is enabled when the answering-machine feature of Phone 1.0 is enabled and is accessed by pressing the 9 key when the phone answers.	(1) Administrator

Assets

Table A-9 lists the assets and describes the data or functionality that Phone 1.0 needs to protect. The table also lists the minimum trust level that should be allowed to access the resource.

Table A-9 Assets

ID	Name	Description	Trust Level
1	Speed-dial list	Contains the names and numbers of frequently used contacts.	(1) Administrator (2) Long-distance user (3) Local call user
2	Caller ID	Provides information about the incoming caller.	(1) Administrator (2) Long-distance user (3) Local call user
3	Access to the PSTN	Phone 1.0 indirectly protects access to the PSTN.	(1) Administrator (2) Long-distance user (3) Local call user

Table A-9 Assets

ID	Name	Description	Trust Level
4	Long-distance calling	Phone 1.0 has optional lockout for long-distance calling so that only authorized users can make long-distance calls.	(1) Administrator (2) Long-distance user
5	Phone configuration	This is the administrative configuration for Phone 1.0.	(1) Administrator
6	Messages	These are messages left by callers when Phone 1.0 has the answering-machine feature enabled.	(1) Administrator (2) Long-distance user (3) Local call user
7	Telephone conversation	The conversation held via Phone 1.0 can contain private information and should be protected.	(1) Administrator (2) Long-distance user (3) Local call user
8	Alertion mechanisms	Includes the audible ringer and flashing LED used to alert the user to incoming calls.	(1) Administrator (2) Long-distance user (3) Local call user
9	Message store	Phone 1.0 stores incoming messages in compressed form on 8 MB of dedicated RAM. The administrator can listen to and delete these messages. The anonymous remote user can leave messages when answering-machine mode is enabled. The message store also houses the outgoing greeting on the phone system.	(1) Administrator (5) Anonymous remote user
10	Outgoing greeting	Phone 1.0 plays this greeting when it answers the phone in answering-machine mode. The administrator has access to change the outgoing greeting. The anonymous remote user hears the greeting when answering-machine mode is enabled.	(1) Administrator (5) Anonymous remote user

Data Flow Diagrams

The Fabrikam Phone 1.0 has two data flow diagrams (DFDs). Figure A-1 shows the context diagram, and Figure A-2 shows the Level 0 diagram. The context diagram depicts the external entities that access Phone 1.0 and its entry points.

The Level 0 diagram shows the data flow for a remote user accessing the administration mode.

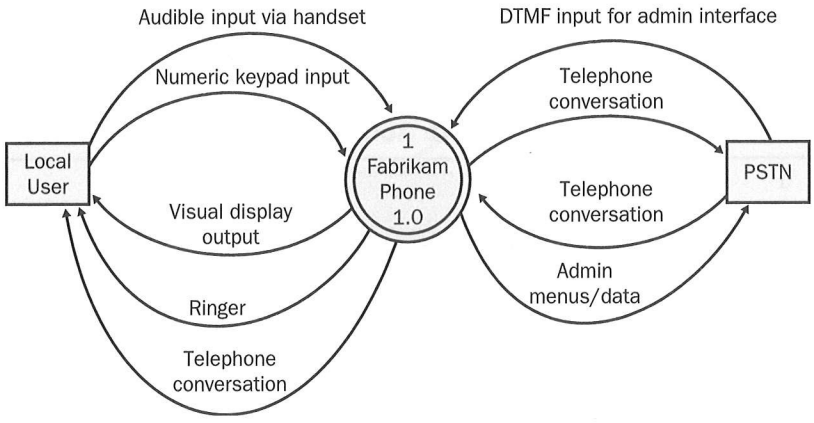


Figure A-1 Context diagram.

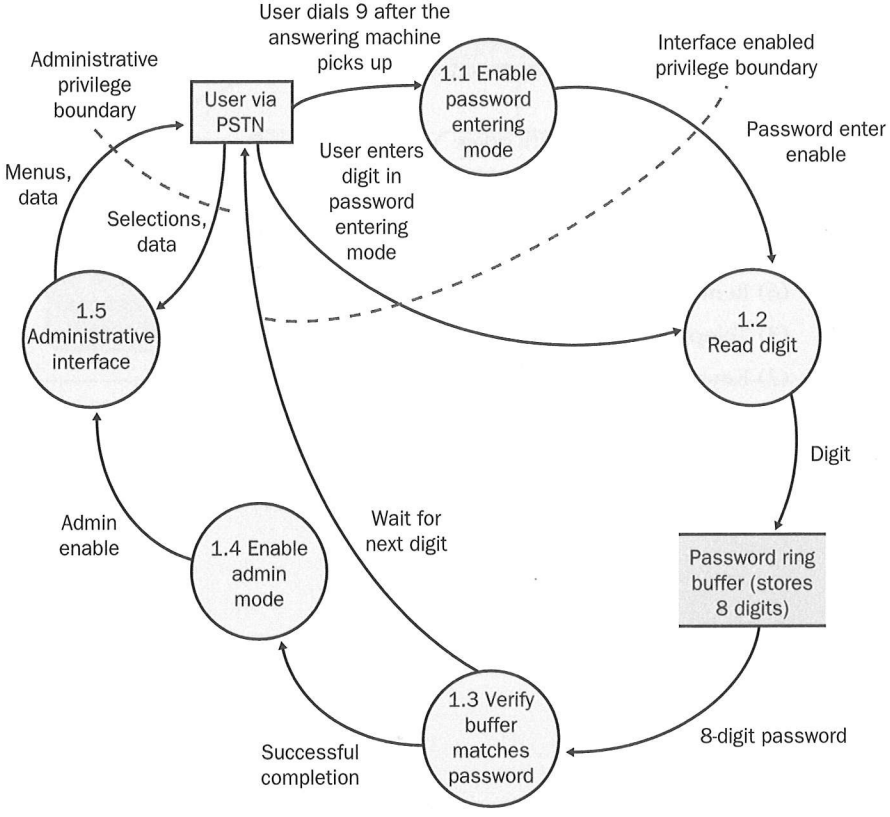


Figure A-2 Level 0 diagram.

Threats

The threats to the application are listed here in a series of tables—one table for each threat. These threats do not imply vulnerabilities. Rather, they are goals that a malicious external entity might have when attacking the system.

Table A-10 Threat: Unauthorized Remote Access

ID	1
Name	Adversary gains access to the remote administration interface, resulting in access to the phone configuration
Description	Phone 1.0 has a remote administration interface that allows an authorized user to configure it via the PSTN. The interface is disabled by default but can be enabled by using the local keypad.
STRIDE classification	■ Tampering ■ Information disclosure ■ Denial of service ■ Elevation of privilege
Mitigated?	No
Known mitigation	If the remote administration interface is enabled, the user should change the default password. *Related external security notes:* (1) Phone 1.0 has a remote administration interface that has a....
Investigation notes	None
Entry points	(6) Remote administration (3) Telephone line (2) Keypad
Assets	(5) Phone configuration

Table A-10 Threat: Unauthorized Remote Access

Threat tree

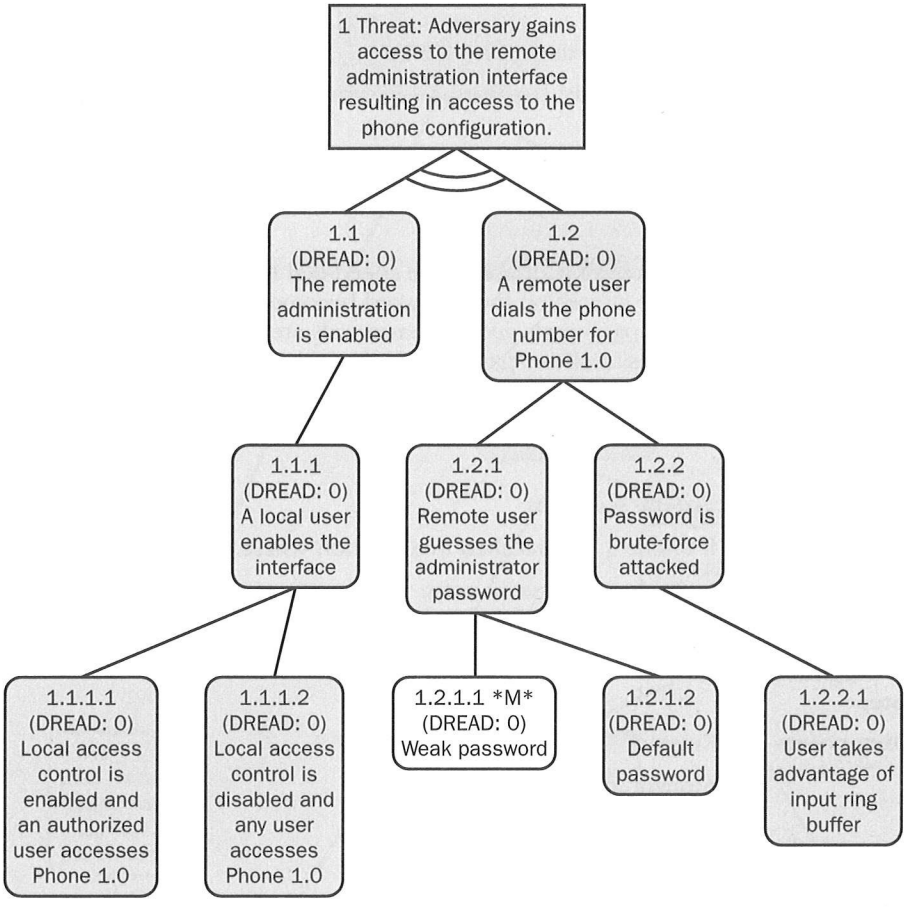


Table A-11 Threat: Speed-Dial List Disclosure

ID	2
Name	Adversary reads the speed-dial list
Description	The speed-dial list has sensitive information (including names and telephone numbers).
STRIDE classification	Information disclosure
Mitigated?	Yes
Known mitigation	If access control is disabled, the speed-dial list cannot be protected. If enabled, brute-force attacks on the password become difficult because the phone requires eight-digit passwords and the passwords are entered via the keypad. Phone 1.0 is not responsible if the password is disclosed by the phone's owner. The threat of an adversary trying to read the speed-dial list via the remote administration interface is covered by the threat of an adversary gaining access to that interface. *Related use scenarios:* (2) If Phone 1.0 is installed in a location where untrusted users can access it.... *Related external security notes:* (2) If the user wants to protect the speed-dial list and whether....
Investigation notes	None
Entry points	(2) Keypad (4) Alphanumeric display (1) Handset
Assets	(1) Speed-dial list

Table A-11 Threat: Speed-Dial List Disclosure

Threat tree

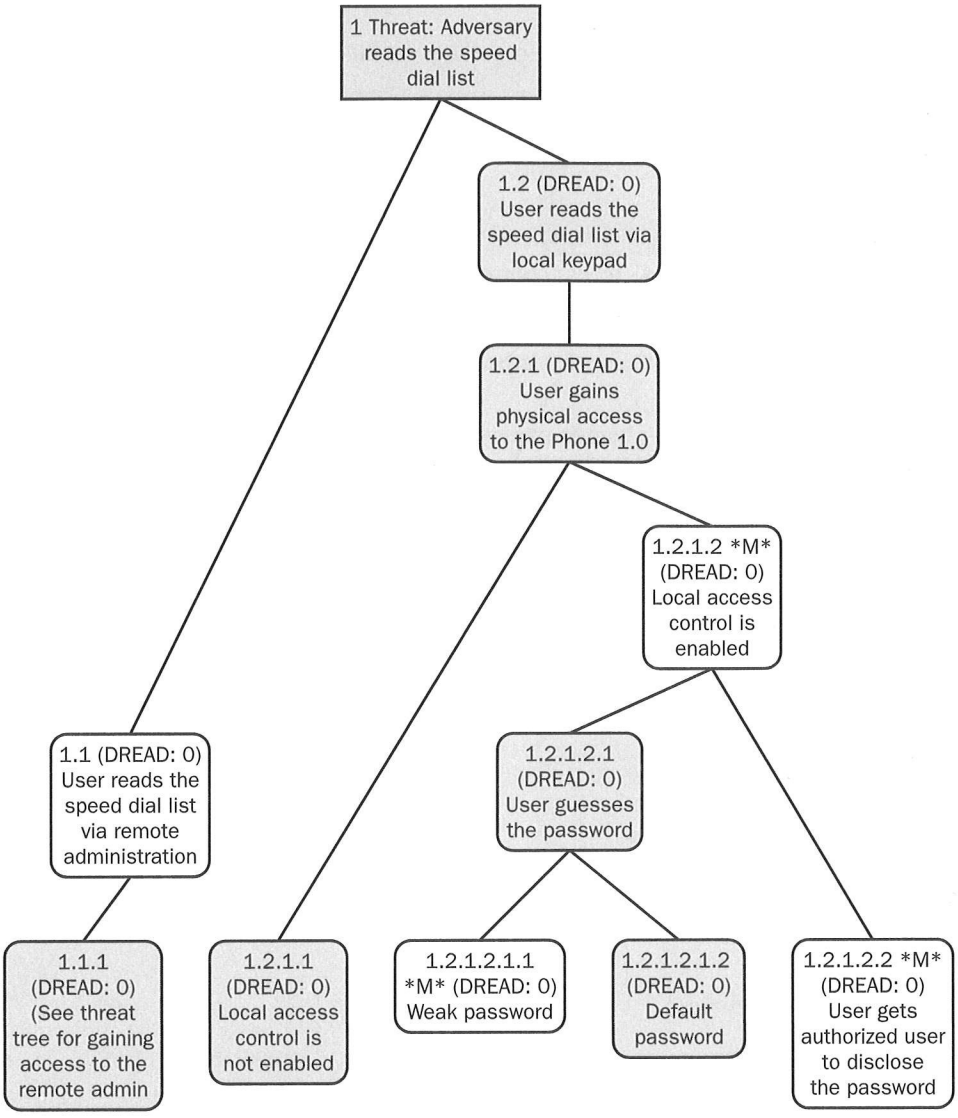


Table A-12 Threat: Unauthorized Long-Distance Call

ID	3
Name	Adversary makes a long-distance call
Description	Access to long distance can be restricted. Often it is not desirable for a company to allow arbitrary users to make long-distance calls.
STRIDE classification	Elevation of privilege
Mitigated?	Yes
Known mitigation	If the local access control is disabled, the long-distance calling capability cannot be protected. If enabled, brute-force attacks on the password become difficult because the phone requires eight-digit passwords and the passwords are entered via the keypad. Phone 1.0 is not responsible if the password is disclosed by the phone's owner. If a long-distance password has not been configured and local access control is enabled, the phone defaults to the local access control password for long distance. Local access control must enabled for a long-distance password to be configured. The long-distance password grants all rights that the local call password does. *Related use scenarios:* (2) If Phone 1.0 is installed in a location where untrusted users can access it.... *Related external security notes:* (3) The long-distance password can be enabled only when local access....
Investigation notes	None
Entry points	(1) Handset (2) Keypad
Assets	(4) Long-distance calling

Table A-12 Threat: Unauthorized Long-Distance Call

Threat tree

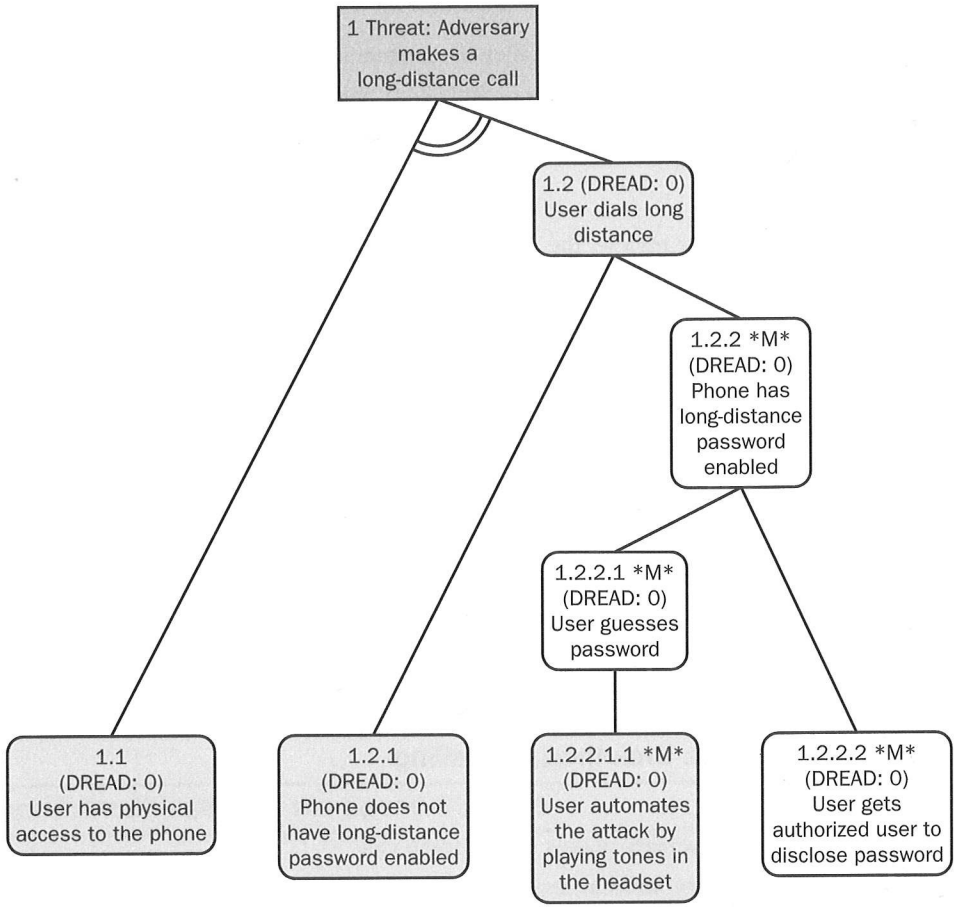


Table A-13 Threat: Disclosure of Caller ID Information

ID	4
Name	Adversary views caller ID information
Description	In some cases, the organization will want to protect caller ID information.
STRIDE classification	Information disclosure
Mitigated?	Yes
Known mitigation	After review, the caller ID information was deemed not sensitive by the threat modeling team. Thus, any user who can view the alphanumeric display can view caller ID data. Given Phone 1.0's current design, the method of protecting caller ID would be to restrict it by using local access control. However, if this method is implemented, the user would have to enter his access code to view the caller ID data for each incoming call.
Investigation notes	To protect caller ID data, Fabrikam would have to use the local access control mode. If this strategy is implemented, the user would have to enter his access code to view the caller ID data for each incoming call. Users likely will not find this requirement user friendly.
Entry points	(4) Alphanumeric display
Assets	(2) Caller ID
Threat tree	None

Table A-14 Threat: Unauthorized Calling

ID	5
Name	Adversary makes an outgoing call
Description	When local access control is enabled, outgoing calls should be restricted to authorized users.
STRIDE classification	Elevation of privilege
Mitigated?	Yes
Known mitigation	Outgoing calls can be restricted only when local access control is enabled. If disabled, the phone has no way to restrict access. *Related use scenarios:* (2) If Phone 1.0 is installed in a location where untrusted users can access it.... *Related external security notes:* (4) If the user wants to control who can make outgoing calls, locate....
Investigation notes	None

Table A-14 Threat: Unauthorized Calling

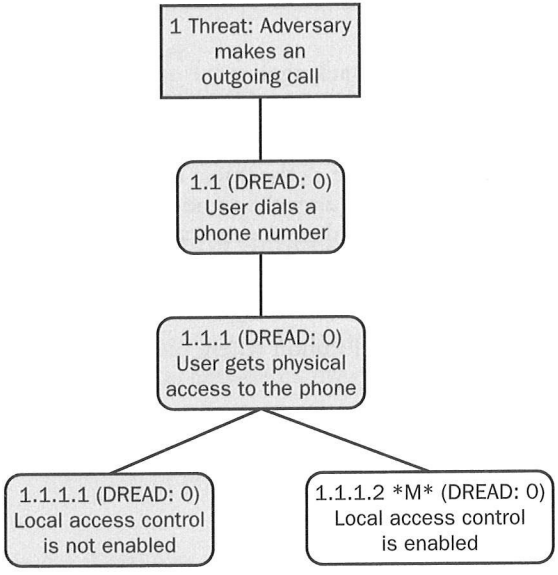
Entry points	(1) Handset (2) Keypad
Assets	(3) Access to the PSTN
Threat tree	

Table A-15 Threat: Modification of the Speed-Dial List

ID	6
Name	Adversary modifies the speed-dial list
Description	If the speed-dial list is modified, an outgoing call could be placed to the wrong number.
STRIDE classification	Tampering Elevation of privilege
Mitigated?	Yes

Table A-15 Threat: Modification of the Speed-Dial List

Known mitigation	The remote administration interface is vulnerable and can unwittingly grant adversaries access to the speed-dial list. See Table A-10, which outlines the threat of an adversary gaining access to the remote administration interface, for the relevant vulnerabilities. Because the security of the speed-dial list depends on the security of this interface, the vulnerabilities of the administration interface are not replicated here. For local access, a brute-force attack against the administrator password requires an adversary to physically press the keypad buttons. Such an attack is significantly more difficult than a remote attack. This threat has the same threat tree as the threat of reading the speed-dial list (outlined in Table A-11) because it requires the same privileges (local call privilege for physical access; administrator privilege for remote) and is accessed in the same manner. *Related use scenarios:* (2) If Phone 1.0 is installed in a location where untrusted users can access it....
Investigation notes	None
Entry points	(2) Keypad (6) Remote administration
Assets	(1) Speed-dial list
Threat tree	None

Table A-16 Threat: Disabling the Ringer

ID	7
Name	Adversary disables the ringer
Description	If the ringer is disabled, the local user will not know when incoming calls are made.
STRIDE classification	Denial of service
Mitigated?	Yes
Known mitigation	See the table's investigation notes. *Related use scenarios:* (2) If Phone 1.0 is installed in a location where untrusted users can access it.... (3) Fabrikam did not design Phone 1.0 to withstand attacks aginst the physical device....

Table A-16 Threat: Disabling the Ringer

Investigation notes	Only an administrator can disable the ringer. Gaining administrative privileges remotely is already covered in Threat 1. An adversary can also disable the ringer by physically opening the phone and cutting the wires leading to the loudspeaker. Because the phone application does not protect against attacks to the physical device, this is not listed as a vulnerability.
Entry points	(5) Audible ringer
Assets	(8) Alertion mechanisms
Threat tree	None

Table A-17 Threat: Conversation Snooping

ID	8
Name	Adversary intercepts a conversation
Description	The conversation between a user of Phone 1.0 and a remote user could be intercepted.
STRIDE classification	■ Information disclosure ■ Elevation of privilege
Mitigated?	Yes
Known mitigation	See the threat tree in this table. The phone was not designed to mitigate against physical attacks (such as implanting a bug), and the security of the PSTN is outside the scope of this threat model. The possible attack of an adversary who is within physical proximity of the phone and overhears a private conversation is also considered external to this threat model. *Related use scenarios:* (1) The Phone 1.0 will be connected to the public switched telephone network.... (3) Fabrikam did not design Phone 1.0 to withstand attacks aginst the physical device....
Investigation notes	None
Entry points	(3) Telephone line (1) Handset
Assets	(7) Telephone conversation

Table A-17 Threat: Conversation Snooping

Threat tree

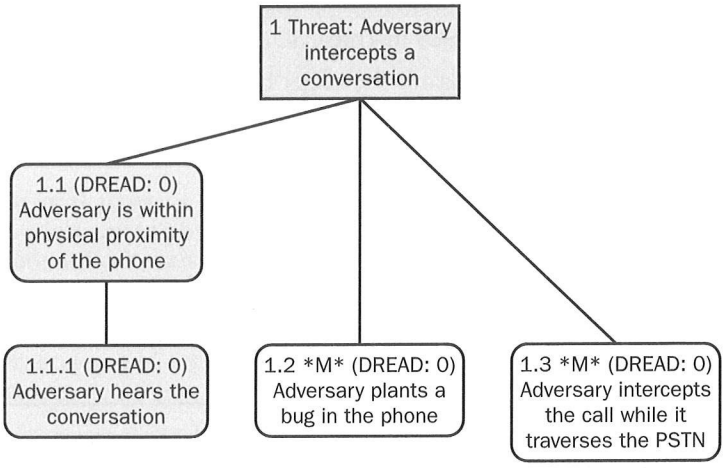


Table A-18 Threat: Message Disclosure

ID	9
Name	Adversary accesses messages
Description	Messages left by callers can contain sensitive information. Access to these messages should be granted only to local authorized users or to remote administrators via the administration interface.
STRIDE classification	Information disclosure
Mitigated?	Yes
Known mitigation	This threat has the same threat tree as the threat of an adversary reading the speed-dial list, depicted in Table A-11. Accessing the messages also requires the same privileges (local call privilege for physical access; administrative privilege for the remote administration interface) as reading the speed-dial list.
Investigation notes	Accessing the messages requires local caller privileges or better, which are granted either locally or via the remote administration interface. Accessing the messages has the same threat tree as that of reading a speed-dial list, as shown in Table A-11.
Entry points	(2) Keypad (1) Handset (6) Remote administration (4) Alphanumeric display
Assets	(6) Messages
Threat tree	None

Table A-19 Threat: Filling the Message Store

ID	10
Name	Adversary fills the message store
Description	A remote user could try to fill the message store so that the owner of Phone 1.0 cannot receive new messages.
STRIDE classification	Denial of service
Mitigated?	No
Known mitigation	None
Investigation notes	None
Entry points	(3) Telephone Line
Assets	(9) Message store
Threat tree	None

Table A-20 Threat: Modification of the Outgoing Greeting

ID	11
Name	Adversary modifies the outgoing message
Description	A malicious user could try to change the outgoing greeting to hurt the reputation or cause other damage to the organization using Phone 1.0.
STRIDE classification	Tampering
Mitigated?	Yes
Known mitigation	See the investigation notes in this table.
Investigation notes	The outgoing message is stored in a fixed location with a fixed size of 128 KB at the end of the 8-MB message store. To change the message, an adversary would have to gain administrative privileges locally or remotely, or she would have to somehow overwrite the buffer holding the message. Because both the outgoing message and the messages left by callers are stored in the message store, an adversary could try to fill the message store and spill over into the outgoing message buffer at the end of the store. However, because this location is fixed, Phone 1.0 employs logic to prevent writing caller messages to this area. To write to this area, the phone must be in administrative mode—meaning that administrative privileges are required to change or delete the message.

Table A-20 Threat: Modification of the Outgoing Greeting

Entry points	(1) Handset (2) Keypad (6) Remote administration
Assets	(10) Outgoing greeting
Threat tree	None

Table A-21 Threat: Deletion of Messages or Speed-Dial Entries

ID	12
Name	Adversary deletes messages and speed-dial information
Description	An attacker could try to delete messages or speed-dial information so that the owner of Phone 1.0 loses important information.
STRIDE classification	■ Tampering ■ Denial of service
Mitigated?	Yes
Known mitigation	This threat has the same threat tree as that of an adversary reading the speed-dial list, shown in Table A-11. In addition, deleting messages and speed-dial information requires the same privileges (local call privilege for physical access; administrative privilege for the remote administration interface) as reading the speed-dial list.
Investigation notes	None
Entry points	(2) Keypad (6) Remote administration
Assets	(1) Speed-dial list (6) Messages
Threat tree	None

Vulnerabilities

The known vulnerabilities of the Fabrikam Phone 1.0 system are listed in this series of tables—one table for each vulnerability. Each table includes the risk associated with not fixing the vulnerability, allowing developers to chose mitigation strategies appropriately.

Table A-22 Vulnerability: User Gains Access to the Administration Interface

ID	1
Name	A user gains access to the administration interface
Description	If the default password is left unchanged and the remote administration interface is enabled, remote anonymous users can easily obtain access to the interface.
STRIDE classification	■ Tampering ■ Information disclosure ■ Denial of service ■ Elevation of privilege
DREAD rating	7.6
Corresponding threat ID	1: Adversary gains access to the remote administration interface, resulting in access to the phone configuration
Bug	432

Table A-23 Vulnerability: Password Brute-Force Attack Against Ring Buffer

ID	2
Name	A user takes advantage of the password ring buffer
Description	If a user takes advantage of the password for the administrative interface being a ring buffer, the attack could take less than 10^8 attempts.
STRIDE classification	■ Tampering ■ Information disclosure ■ Denial of service ■ Elevation of privilege
DREAD rating	3.8
Corresponding threat ID	1: Adversary gains access to the remote administration interface, resulting in access to the phone configuration
Bug	443

Table A-24 Vulnerability: Filling the Message Store

ID	3
Name	Adversary repeatedly leaves messages on the phone, filling the message store
Description	An adversary can repeatedly call the Phone 1.0 application and leave repeated messages, thereby filling the message store. Because messages can be up to 60 seconds long, an adversary can fill the store quickly. Once the store is full, no more messages can be received. For mitigation, Fabrikam might add a throttling based on caller ID information that can be enabled or disabled via the administration interface.
STRIDE classification	Denial of service
DREAD rating	6.4
Corresponding threat ID	10: Adversary fills the message store
Bug	478