Threat Modeling Challenge

Company Background:

Forderly is the premier solution for your small business food ordering needs. Our patent-pending technology and state-of-the-art hardware platforms allow any restaurant to streamline their food ordering and delivery processes to enhance your customer's in-restaurant experience. Our early stage startup is backed by some of the biggest luminaries in the venture capital market and we are poised to be the next "unicorn" in the food industry.

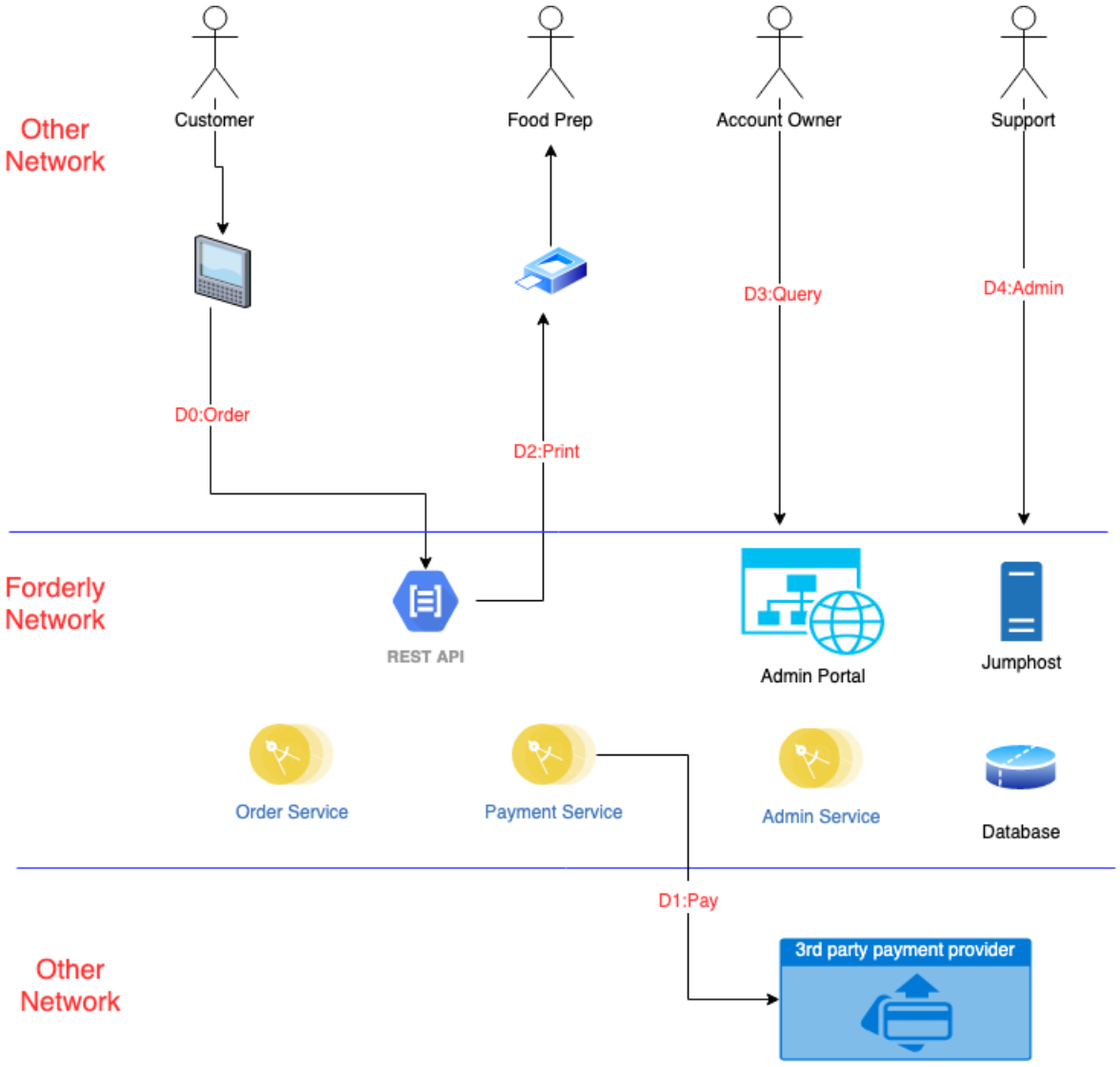
Application

Our multi-tenant SaaS platform and custom-built ordering and printing platforms provide our customers with the scale and service required for the largest processing requirements. All of this is built using a distributed application services backbone and hosted in our state of the art co-location facilities.

Core Technologies Info

1. Kiosk - Hardened version of SELinux deployed into a custom built tablet that is locked down to only include touch screen and wireless ("wi-fi") connectivity. Each kiosk is maintained through a phone-home features which constantly updates the device with the latest features and security patches. Kiosks take configuration centrally from our SaaS.
2. Administrative Website - Our administrative portal provides customer administrators the ability to query their daily sales and produce reports using a streamlined UI built using the Angular technologies supporting a robust set of REST apis.
3. Microservices - Our core services are written in Java and communicate via REST api calls. There are 3 main services
    a. *Order service* - Processes a customers order
    b. *Payment service* - Transacts with the outside payment provider to charge the customer's credit card
    c. *Admin service* - Allows the customer's administrator to manage Kiosk and Printer devices, configure menu items (name, description, cost), and produce reports (i.e. order history, customer feedback, daily/weekly sales info, etc)
4. Database - Our core database is a Postgres version 11.4 database
5. Printer - Our printer is a custom-built dot matrix printer that prints carbon-copy receipts and is connected via ethernet using DHCP to poll for orders to print.
6. SSH- Forderly support staff use SSH to connect to our hosted environment. Forderly uses standard OPENSSH for this connection.
7. Payment Processor - Our services leverage a reputable external payment processor. This component is not directly in scope for this Threat Model but communication with it is in scope. The Payment Processor is a PCI certified vendor.

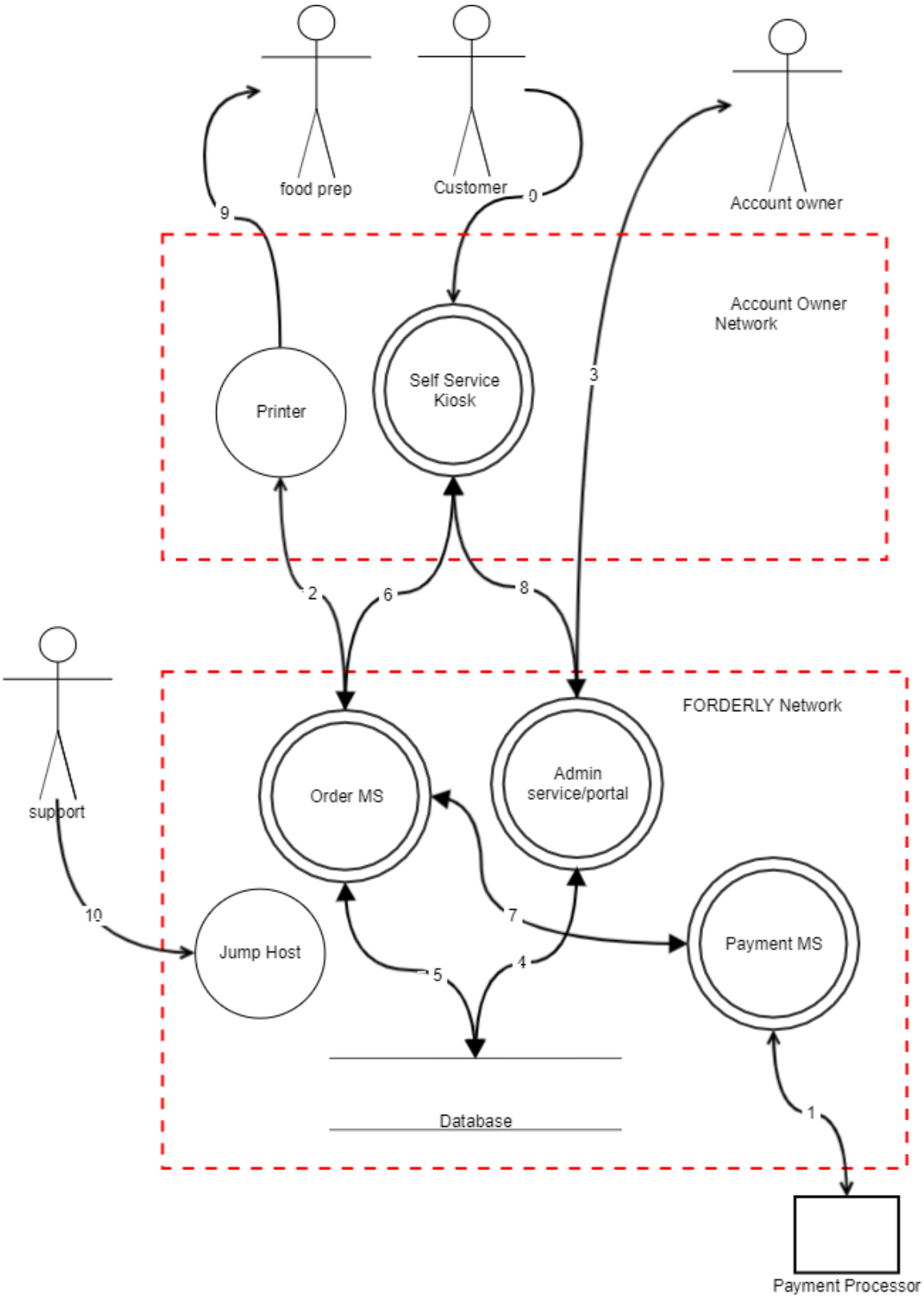
Marketing Architecture Diagram



Descriptions of process flows

Id	Name	Description
D0	Order	**Customer Order**: Customer selects desired food items via touchscreen on the kiosk. Once they accept, the kiosk sends the preliminary order via the rest api to the order service which writes it to the database under the tenant Id of the customer. The rest api then communicates back to the kiosk to have the customer swipe their credit card. Customer swipes the card and the kiosk sends the information via the REST api to the admin service which calls the payment service (See D1 for details). Orders are then printed (See D2 for details). Once the food prep folks receive the order, they prepare the food and deliver it to the customer.
D1	Pay	**Process Credit Card**: The payment service then contacts the 3rd party payment provider with credit cards details via their api and the processor provides a token back to the payment services. The payment service then writes the payment token to the database and releases the order for delivery to the food prep staff
D2	Print	**Order Print**: The printer periodically wakes up and queries the order service via the REST api looking for new orders to print. If it receives one, it prints the order out and informs the order service it is printed. The order service then updates the database with the current state. Each printer has a unique GUID. This is used to associate the printer with a SSK and is how orders are routed to the right printer
D3	Query	**Customer Administration**: The customer administration portal allows customer users to login via a password and perform the following tasks. ● Review pre-canned reports ● Provision/Deprovision kiosks to their account ● Configure Kiosks a. Associate Kiosks and Printers b. Setup food menus on the machine c. Remotely update kiosks with latest patches/firmware ● Provision/Deprovision account users ● Configure menu items (name, description, cost) Each of these tasks are accomplished by the admin portal in a standard web manner. All actions are maintained and logged in the database.
D4	Admin	**Privileged Access**: A Forderly Support and Operations team login into the Jump host via SSH key. Once logged in, the support person can then access all of the machines co-located within the Forderly production network via SSH

Forderly System Data Flow Diagram prepared by the development team



Annotations

0 Customer to Self Service Kiosk	
Description	Customers interact with the SSK via a touch screen to order food, pay for their meal and leave customer feedback. They have a free form text field where they can type in feedback on service and food quality. The max length of this field is 1024.
Encryption	N/A
Authentication	N/A
Other	The kiosk is owned by Forderly and leased by the food provider

1 Payment Service to Payment Processor	
Description	The Payment processing service communicates with the external entity for processing credit card payments via a REST call using a published API
Encryption	TLS 1.2
Authentication	Mutual Authenticated TLS connection where both sides have properly exchanged keys.
Other	

2 Printer To Order Processing service	
Description	Printer periodically polls the order service using its unique GUID. if an order exists, it prints it out and notifies that the printed order was successful. Each printer has an embedded GUID, using this GUID the printer is provisioned to a customer account. The customer admins can associate SSK and printers via the Admin portal.
Encryption	HTTP because non-sensitive information traverses this channel. No credit card or PII in this channel.
Authentication	Printer authenticates to order processing service using the GUID of the printer.
Other	

3 Account Owner to Admin Service/Portal

Description	Account owner interacts with the Administrative portal to perform the following tasks. ● Review pre-canned reports ● Provision/Deprovision kiosks to their account ● Configure Kiosks a. Associate Kiosks and Printers b. Setup food menus on the machine c. Remotely update kiosks with latest patches/firmware ● Provision/Deprovision customer users ● Configure menu items (name, description, cost
Encryption	TLS 1.2
Authentication	Username and Password
Other	

4.Admin service to Database	
Description	All communication between the Admin service to the DB happens via a JDBC connection.
Encryption	TLS 1.2
Authentication	Admin service has hard-coded credentials to the database using the admin account
Other	

5 Order service to Database	
Description	The order service DB communication is coded in legacy Java code without a JDBC driver . All communication is done by a TCP/IP internal library that mimics a command-line client to the database.
Encryption	Self-designed cipher
Authentication	Order service picks up credentials from db_creds.txt on its filesystem, logs in as admin
Other	

6 Self Service Kiosk to Order Service	
Description	1. The Kiosk communicates order and payment information to the order services to process the order. 2. The order service responds with order and payment details. 3. Order Feedback information is written to the DB from here.
Encryption	TLS 1.2

Authentication	Each Kiosk is provided with a RSA 2048 Certificate that is generated when the machine is manufactured.
Other	

7 Order service to Payment Service	
Description	All communication between the Payment service Order Service is done via Rest. This channel is used to pass payment information from the SSK to the payment service.
Encryption	None
Authentication	None
Other	

8 Self Service Kiosk to AdminService portal	
Description	SSK makes calls to the AdminService portal for 2 use cases: 1. Retrieve latest SSK configuration when modified by an Admin User. 2. Retrieve the latest SSK software binary to upgrade the SSK.
Encryption	TLS 1.2
Authentication	Each Kiosk is provided with a RSA 2048 Certificate that is generated when the machine is manufactured
Other	Each Kiosk has a unique certificate.

9 Food Prep person to Printer	
Description	Food prep person receives a printed order slip used to prepare the order.
Encryption	None
Authentication	None
Other	The order # is printed on the order slip. There is no credit card information on the order slip.

10 Support to Jump Host	
Description	Forderly Support and Operations team access the environment via a jump host. System is a Linux based Operating System. Users connect via SSH.

	Access to this network is restricted by a firewall. It only allows in and outbound connections for the 3 services over 443.
Encryption	SSH
Authentication	Users authenticate using “supportuser” via an SSH Key
Other	Arrows were left out for diagram simplicity. Once Support and Operation personnel connect to the Jump Host they are able to connect to internal system via SSH. SSH keys for service hosts are stored in “supportuser” account on the Jumphost. DB credentials stored in private /home/supportuser/.db/credentials file on the Jumphost.

Fooderly Trust Boundary	
Description	Access to this network is restricted by a firewall, which represented by the dotted red line for the Forderly Production Network. It only allows the following rules: INBOUND 443 to AdminServicer/Portal and Order Service INBOUND 22 to Jump Host OUTBOUND 53 DNS OUTBOUND 443 from Payment Service to Payment Processor.
Other	