EECS 159A/CSE 181A
Refinement of Communication

Outline

- Realistic Constraints
  - Regulations: Privacy
  - Budget: Cost, Power
- Iterative design process
  - Defining interfaces between subsystems
  - Top-down and bottom-up refinement

Top-down vs Bottom-up

- Top-down refinement
  - Expand high-level ideas into details
  - Ensure user issues are specified
- Bottom-up design
  - Pick concrete components and connect them
  - Ensure required function can be realized
- Need to iterate between both!
  - Check constraints as more details become available

What we’ve done so far

- Exploration stage
  - top-down: refine application ideas
  - bottom-up: explored technology options
- Design stage
  - top-down: expand block diagrams & flowcharts
  - bottom-up: layers of communication stack
- Top-down again, but with the broader considerations
  - e.g., security & privacy

Data from the Scanner

- Depends, but normally it's just ASCII data
  - 3 Tracks of data, emulates a keyboard device
- Sample data (text string)

  -
    ```
    %B60383800<u>12345678</u>^ANTEATER/PETER Z
         ^491212000000000    000   ?;
    6038380006514029=49121200000000000000?
    ```
  - just need to extract the <u>8-digit ID</u> and <u>name</u>
  - comes in on the serial port (UART)

Private vs Public info

http://www.reg.uci.edu/services/verifications/infoverified.html

Private	Public
student ID number	**student's name**
social security number	address (campus email, local, and/or permanent) and telephone numbers
GPA	date and place of birth
grades	major field of study, dates of attendance, number of course units in which enrolled, degrees and honors received
number of units completed	class level
courses taken in the past or in progress	enrollment status (e.g., ugrad or grad, full-time or part-time)
student's schedule	photo
residency classification	most recent previous educational institution attended
status of application for graduation	participation in officially recognized activities, including intercollegiate athletics
	name, weight, and height of participants on intercollegiate university athletic teams

UCI Policy on private info

- Private information will only be verified with student authorization
- Student authorization consists of:
  - valid photo ID presented by the student when making a verbal verification request or when requesting a "hand carry" verification
  - student's signature on a mailed verification request
  - a letter signed by the student including the specific name of the person authorized to obtain the verification on their behalf
  - The authorized person must present a valid photo ID. Therefore "my mom" or "my friend" will not be sufficient.

Federal Laws on Data Privacy

- FERPA
  - Family Educational Rights and Privacy Act
  - a Federal law that protects the privacy of student education records
- HIPAA
  - The Health Insurance Portability and Accountability Act (1996)
  - a Federal law that, among other things, protects the privacy of individually identifiable health information

UC Electronic Communication Policy

- http://policy.ucop.edu/doc/7000470/ElectronicCommunications
- Section V.E: Encryption
  - Where deemed appropriate, electronic communications containing **restricted data** as defined in Business and Finance Bulletin IS-3, Electronic Information Security **should be encrypted** during transit across communications networks. Other communications may be encrypted during transit. All encrypted communications shall be handled upon receipt in conformance with the storage requirements for electronic information resources, as defined in IS-3.

IS-3: Electronic Information Security

- http://policy.ucop.edu/doc/7000543/BFB-IS-3
- Restricted Data
  - The proliferation of data greatly increases risks of unauthorized access, particularly when data is stored in ad hoc analysis tools such as spreadsheets and desktop databases. When data is copied for analysis or research, restricted data should be **deleted whenever possible** or "**de-identified**" by removing data elements that, in combination with other data, would result in the identification or description of an individual. If it is not possible to delete restricted data, adequate security measures must be implemented. Note that restricted data is one form of restricted resources as defined in this bulletin.

Policy on Restricted data on Portable Devices

- http://policy.ucop.edu/doc/7000543/BFB-IS-3
    - Section 3.e: Restricted information may be retained on portable equipment **only if protective measures, such as encryption, are implemented** that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment (see III.C.2.g, Encryption above).

Options for handling restricted information

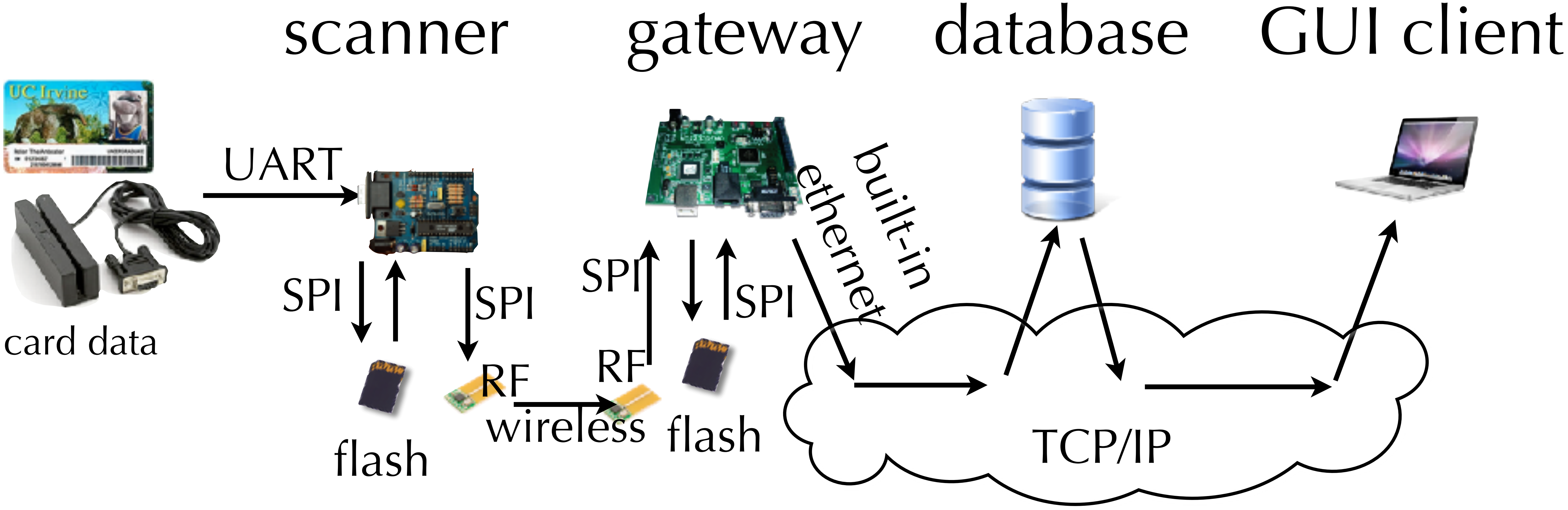
- If you transmit & store student ID#
    - encryption is necessary during transmission
    - encryption is necessary for storage on portable
- If you don't transit or store student ID#
    - need another way to map identity to some identifying string (that is not the student ID#)
    - need a way to map this identifying string back to student ID#

Crypto methods

- “Irreversible” (unless by brute force)
  - hashing (e.g., MD5, SHA, …)
  - can use a hash key, salt (additional noise), …
  - Good for storing restricted data that you just want to check (e.g., password, student ID)
- Reversible (encrypt & decrypt)
  - Symmetric key (“secret key”, e.g., AES)
  - Asymmetric key (“public-private key” e.g., RSA)
- Stream vs Block Encryption

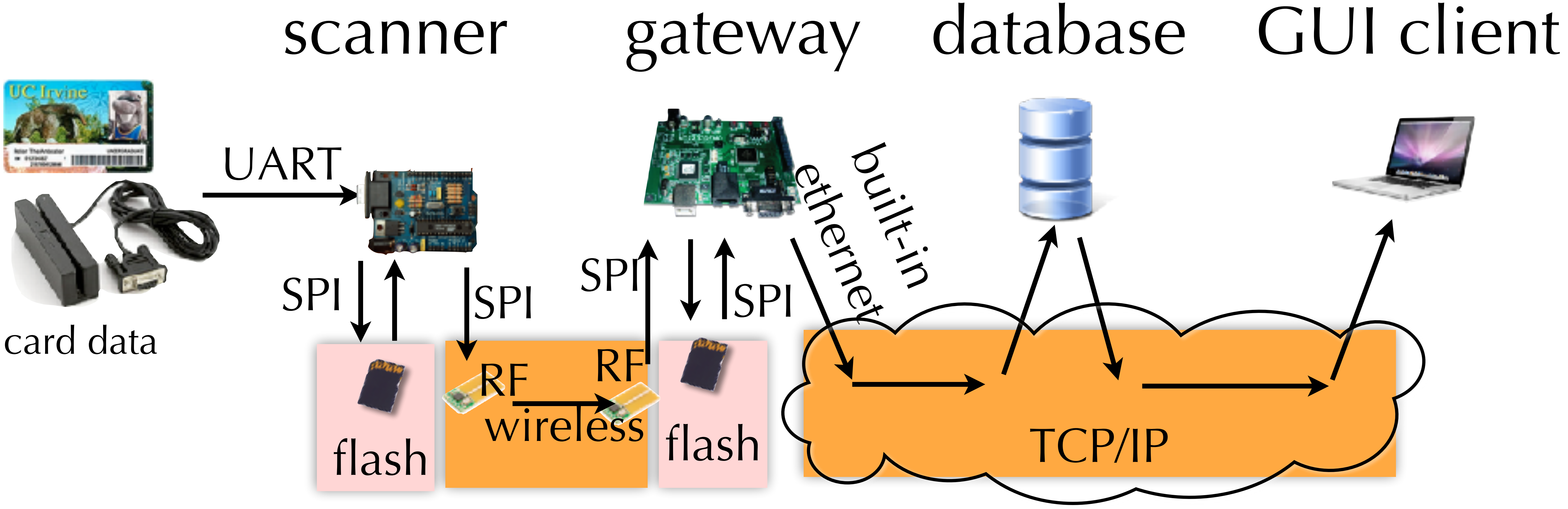
Block diagram from last time

- Given: high-level blocks with links
- Task: refine the meaning of those links
  - i.e., define the protocols
  - not just for communication, also for control



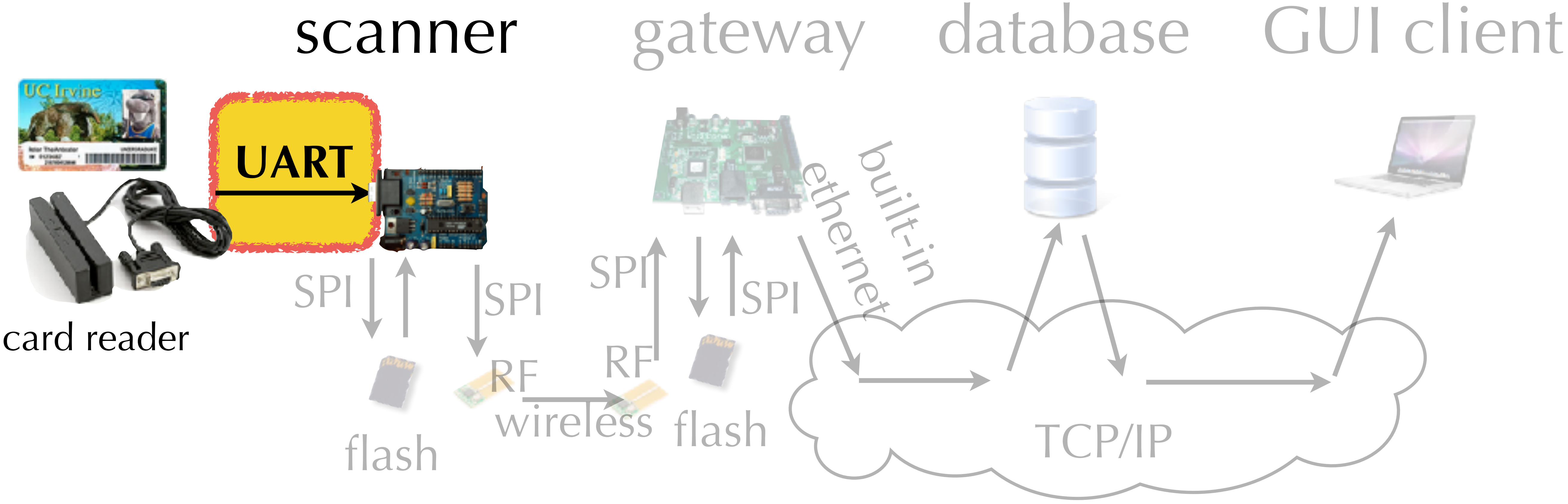
Encryption vs Secure Channel

- Data stored on flash memory
- Data transmitted over external network
  - unencrypted data over secure channel, or
  - encrypted data over insecure channel



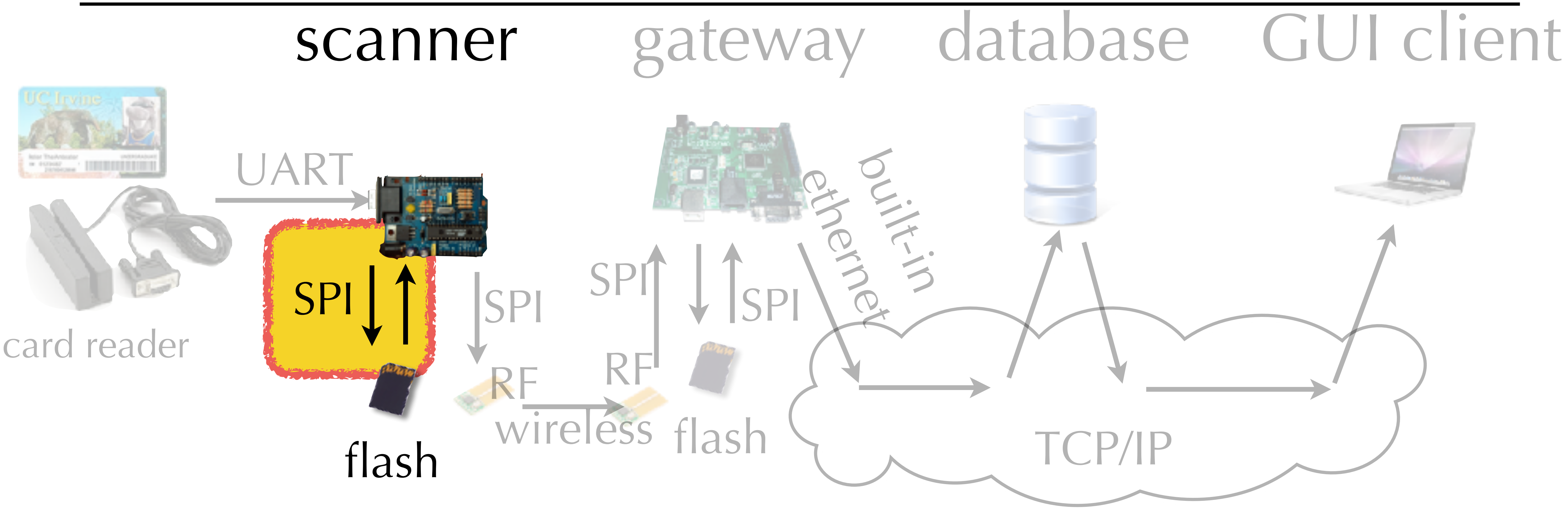
Card-reader to MCU

- Transport: UART
- Format: text stream
- Encryption: none
  - this is ok, because it is transient & can't be snooped



MCU to/from flash

- Transport: SPI
- Format: encrypted block text?
- Encryption: by MCU
  - what encryption algorithm? Does MCU decrypt?



Data to log to flash

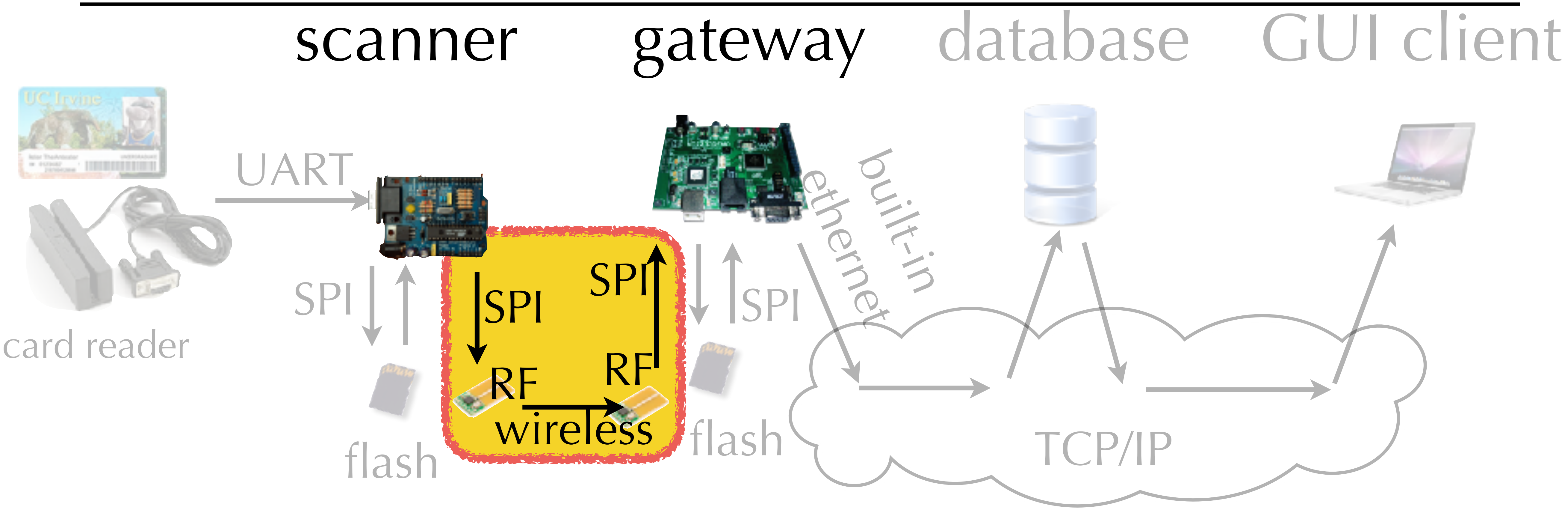
- What data to log?
  - Student ID? Name? Expiration date? Time stamp?
  - As text string? As a binary struct?
  - How many samples to buffer before logging? (flash memory is page based)
- Encrypt
  - What method? 1-way or 2-way?
  - What to encrypt? All data or just restricted data?

Crypto choice for logging

- Suitable choices
  - Hash (e.g,. MD5)
  - Symmetric-key encryption
- Reasons
  - lower complexity compared to asymmetric keys
  - Assumption: the crypto key is not easily exposed or guessed
- Asymmetric key crypto would be overkill

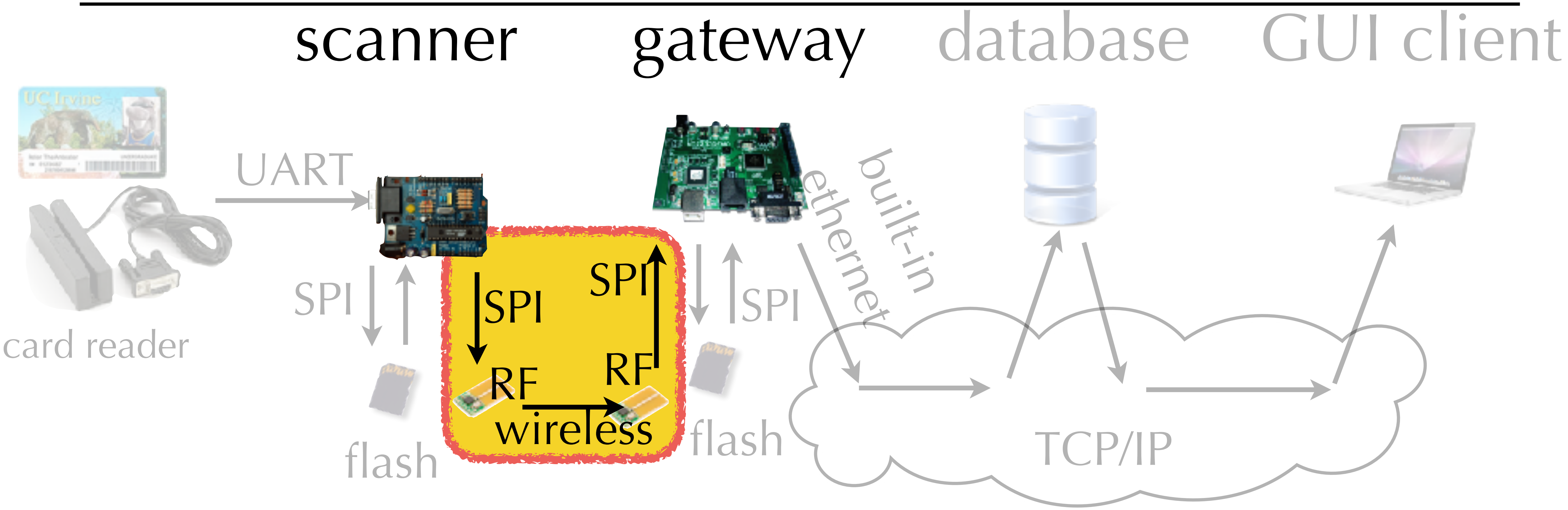
Scanner to Gateway

- Transport: some wireless interface
- Style: Push by Scanner or Pull by Gateway?
- Encryption:
  - depends on what you do to data from flash memory



Scanner to Gateway

- if we don't decrypt data from flash
  - can send directly without encrypting again! (ok to encrypt)
- if we decrypt data from flash
  - either must encrypt data again before transmitting,
  - or must use secure channel to transmit restricted data



Encryption capability of different Wireless Modules

Level	Concept	AM radio	TR 1000	CC 1000	CC 2420	CC 2530
Application	behavior					
Profile	format					protocol stack (software)
Network	topology					
Data Link	connection					
MAC	packets				v	v
PHY	bytes			v	v	v
PHY	bits		v	v	v	v
PHY	volts	v	v	v	v	v

hardware
software
either

unencrypted transport

=> MCU responsible for encrypting before Tx, decrypting after Rx

module has built-in crypto hardware

=> hardware **can** encrypt before Tx, decrypt after Rx

Multiple access

- Allow multiple radios to share bandwidth
  - Not all transceivers support MA at MAC level
  - MAC could be controlled by software
- Styles
  - FDMA: separate channels (expensive: multi-radio)
  - TDMA: use time slots (Bluetooth, w/ master-defined frequency hopping sequence)
  - CSMA: (Ethernet, Wi-Fi, 802.15.4)

Example: CC2420 — CSMA

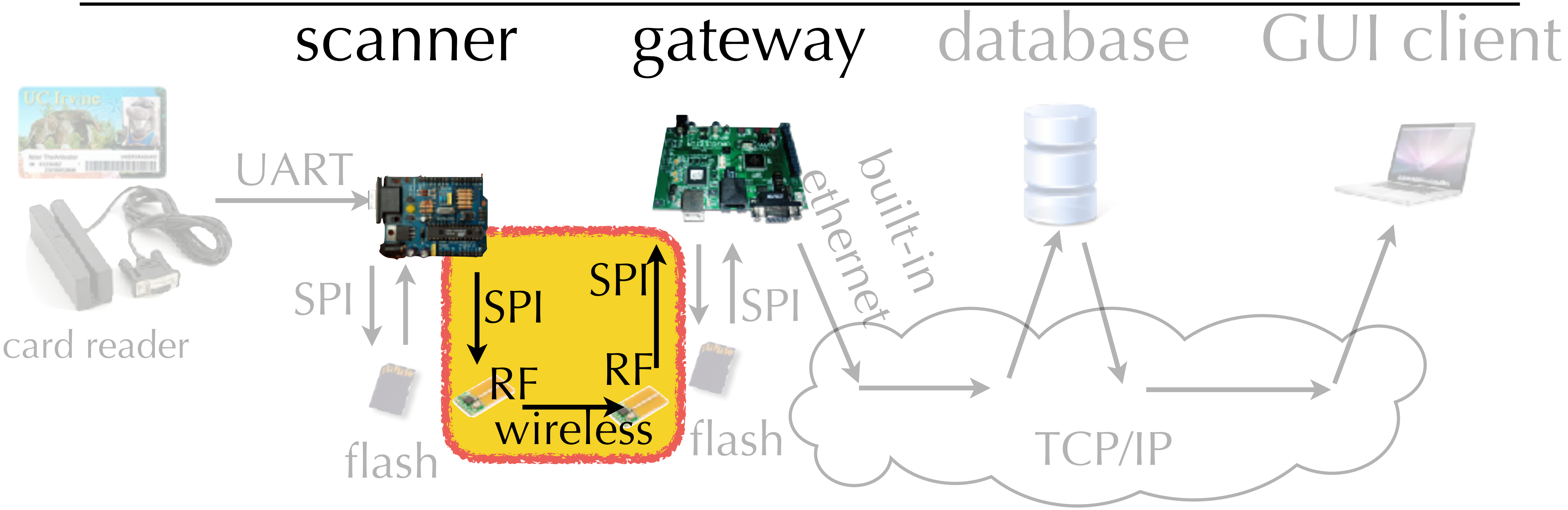
- Carrier-Sense Multiple Access
  - “Clear-Channel Assessment” (CCA) before Tx
  - if channel occupied, backoff for random time
- Advantages
  - short latency if channel utilization is low
  - effective for power managing transmitter (Tx)
- Disadvantage
  - receiver (Rx) must be alway on
  - inefficient when channel is more utilized (more collision)

Example: nRF24L01 (Enhanced Shockburst)

- Each node has a configurable ID
- Transmitter
  - No carrier sense or RSSI. Just send.
  - Hardware adds receiver ID before payload
- Receiver
  - Need to be in Rx mode to receive.
  - Hardware can match up to 6 IDs, discard if not matched
- Support for reliable communication
  - hardware auto-ACK and auto-ReTx

Scanner to Gateway

- Push by scanner?
  - Scanner has data => push to gateway
- Pull by gateway?
  - Gateway periodically queries scanners

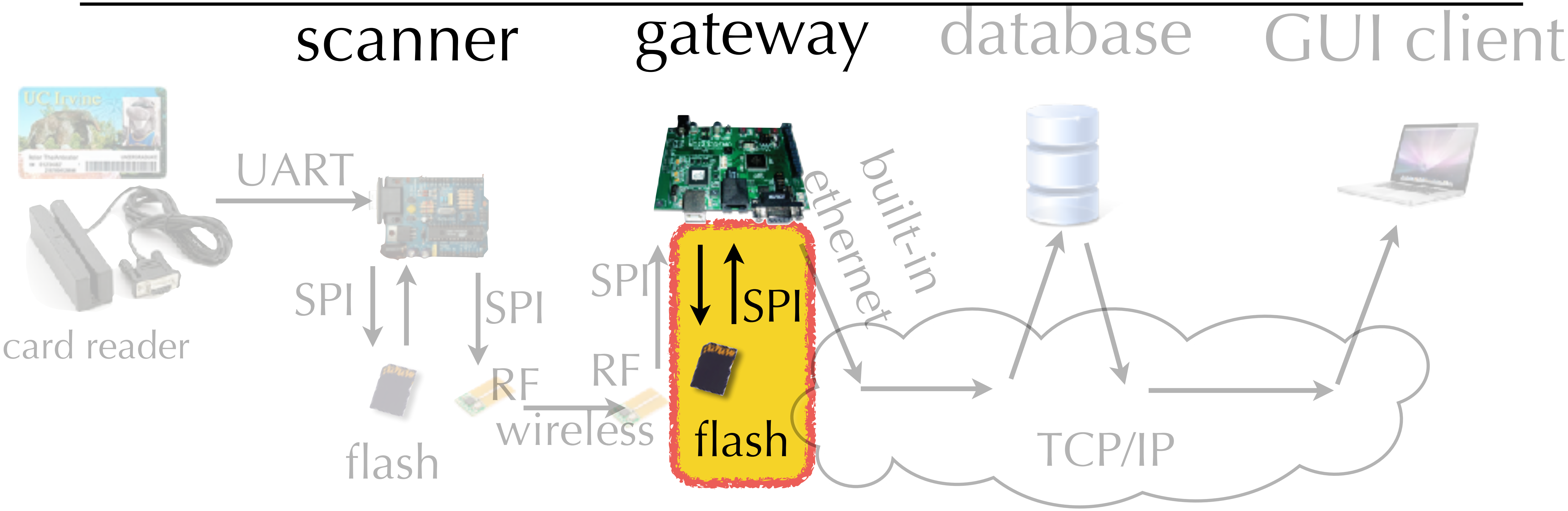


Two styles of network formation

- Scanner-initiated ("pushing")
  - scanner requests connection to gateway
  - issue: contention among scanners
- Gateway initiated ("pulling")
  - ask each scanner if it wants to connect
  - one gateway => no contention
    (but multiple gateway could contend)
  - may take long time to enumerate addresses

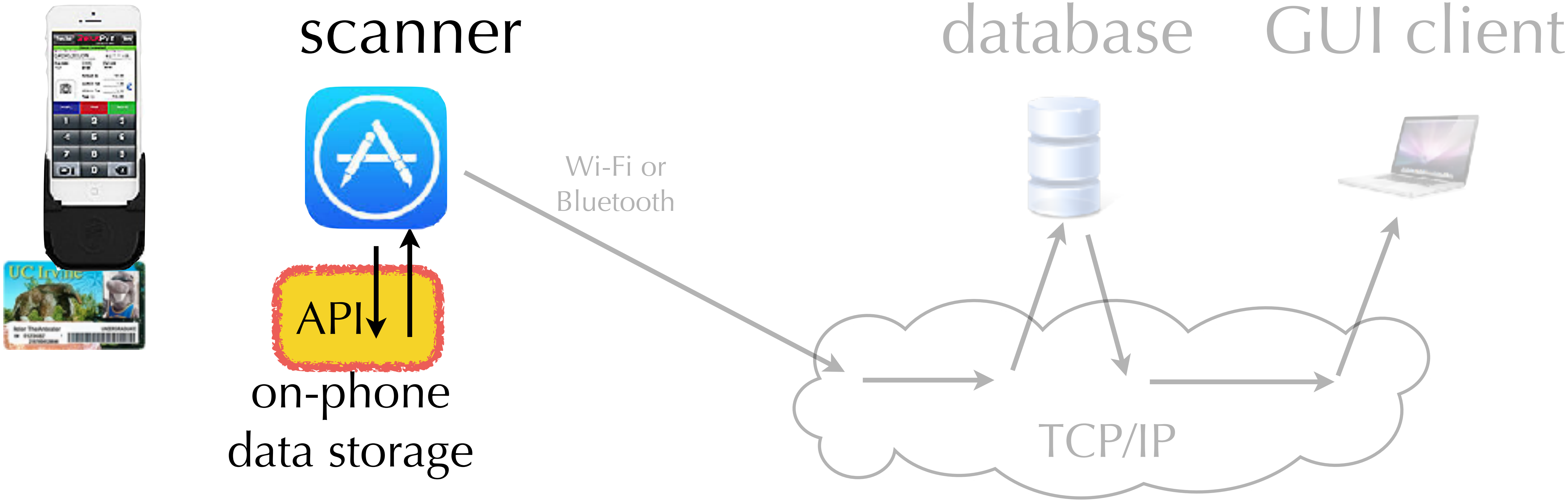
Gateway to log to flash

- no need to encrypt if payload already encrypted
- if wireless module decrypts, MCU needs to encrypt again



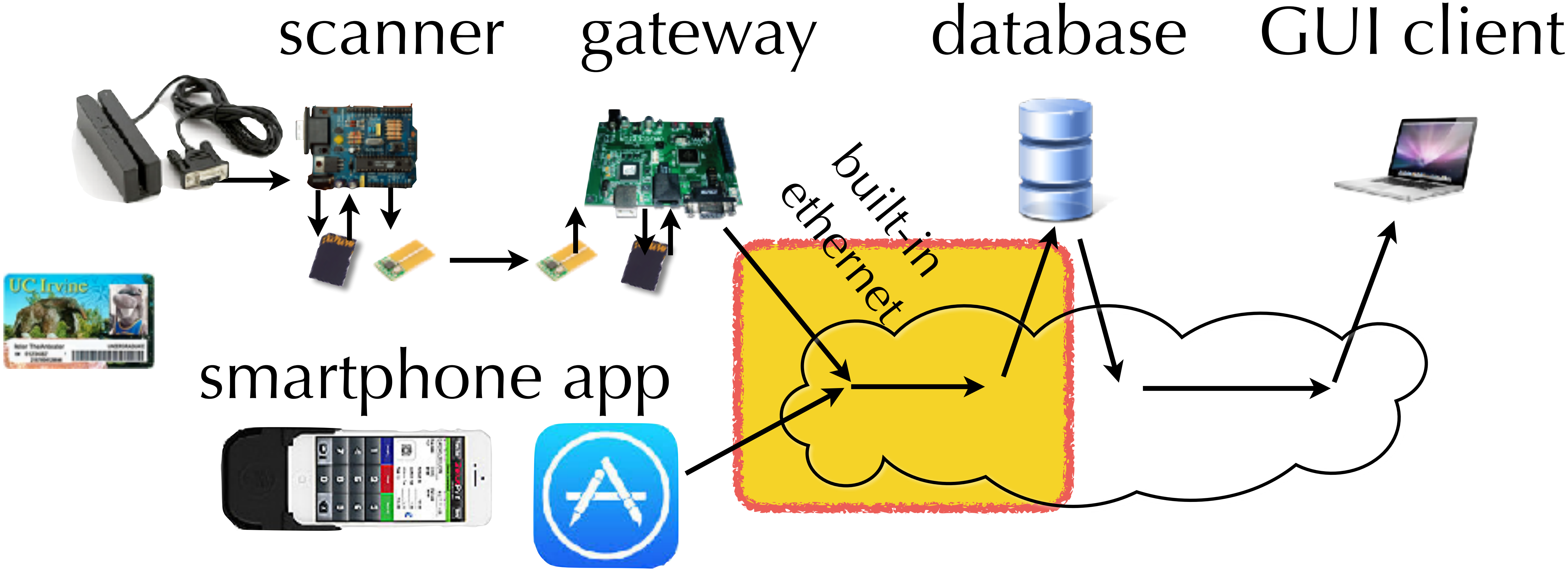
Need for Encryption on Mobile

- e.g., scanner as a smartphone app
  - Still need to store restricted data in encrypted form
- Encryption done by
  - app itself to unencrypted storage
  - data storage (on phone) could support encrypted storage



Gateway or Phone to Server

- Transport: over the Internet
  - e.g., HTTP (insecure), HTTPS (secure)
  - Need to define the format of message & reply



Possible protocol: HTTP

- Protocol used in web client-server on top of TCP/IP
- Request (from client to server)
  - Header
    - First line: a “verb” followed by arguments (e.g., URL)
    - Additional lines of attributes (key-value pairs)
  - Body (after the header and a blank line)
    - Some verbs can have additional data in the body section
- Reply (from client to server)
  - Header: OK, error (e.g., page not found, etc)
  - Body: additional data for some verbs

HTTP verbs

- GET
  - by default when you load a web page
  - Example client message to server: (header only)

    ```
    GET /index.html HTTP/1.1
    Host: www.uci.edu
    ```
- POST
  - often when you fill out a web form
  - the key=value pairs are given in the body. e.g.,

    ```
    id=25d55ad283aa400af46476d713c07ad&expire=2009
    92&event=eecs-advising-20091204&time
    stamp=20091204T0930Z
    ```

Gateway-Database Transaction Format

- https://eee.uci.edu/09f/18160/homepage/Transaction+format.pdf
- Client (Gateway) POST to server over http

element	description	example
id	Student ID MD5 encrypted.	25d55ad283aa400af464c76d713c07ad
expire	6 digit term expiration	200992
event	Identifier of event to attach student transaction to.	eecs-advising-20091204
timestamp	In order to work safely in URIs, an ISO 8601 combined UTC timestamp using basic time format.	20091204T0930Z

```
POST /process_id.php HTTP/1.1
Host: foo.eng.uci.edu
User-Agent: Mozilla/5.0
Content-Length: 103
Content-Type: application/x-www-form-urlencoded

id=25d55ad283aa400af464c76d713c07ad&expire=200992&event=eecs-
      advising-20091204&timestamp=20091204T0930Z
```

Server Response

element	description	example
id	Student ID MD5 encrypted.	25d55ad283aa400af464c76d713c07ad
result	Result code	ok

```
HTTP Status Code: HTTP/1.1 200 OK
Date: Fri, 04 Dec 2009 04:59:42 GMT
Server: Apache/1.3 (Unix) mod_ssl/2.8.28 OpenSSL/0.9.8f
Connection: close
X-Powered-By: PHP/5.2.11
Last-Modified: Sat, 14 Mar 2009 08:36:36 GMT
Content-Length: 45
Content-Type: text/csv;

id=25d55ad283aa400af464c76d713c07ad&result=ok
```

HTTP vs HTTPS

- HTTP
  - unencrypted channel
  - snooper can see the entire message in text
  - quick to connect & respond
- HTTPS
  - secure channel (encrypted)
  - takes time to establish transport-layer security
  - entire request and response are encrypted

Other Realistic Constraints

- Security
- Privacy
- Economic
- Environmental
- Social
- Political
- Ethical
- Health and Safety
- Manufacturability
- Sustainability
- Standard compliance