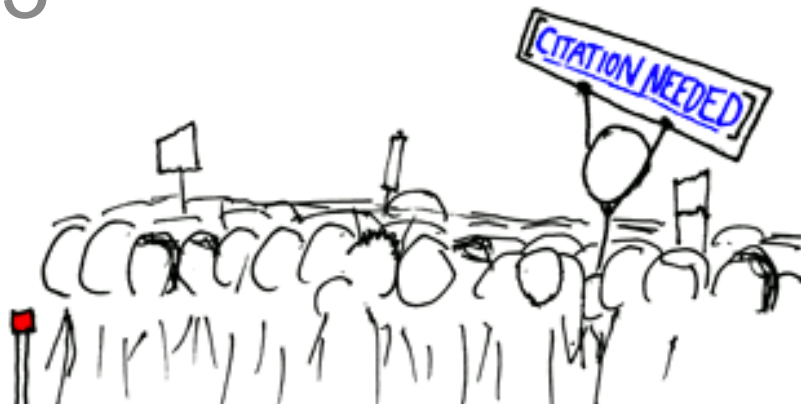
Security and Privacy

Lecture 13

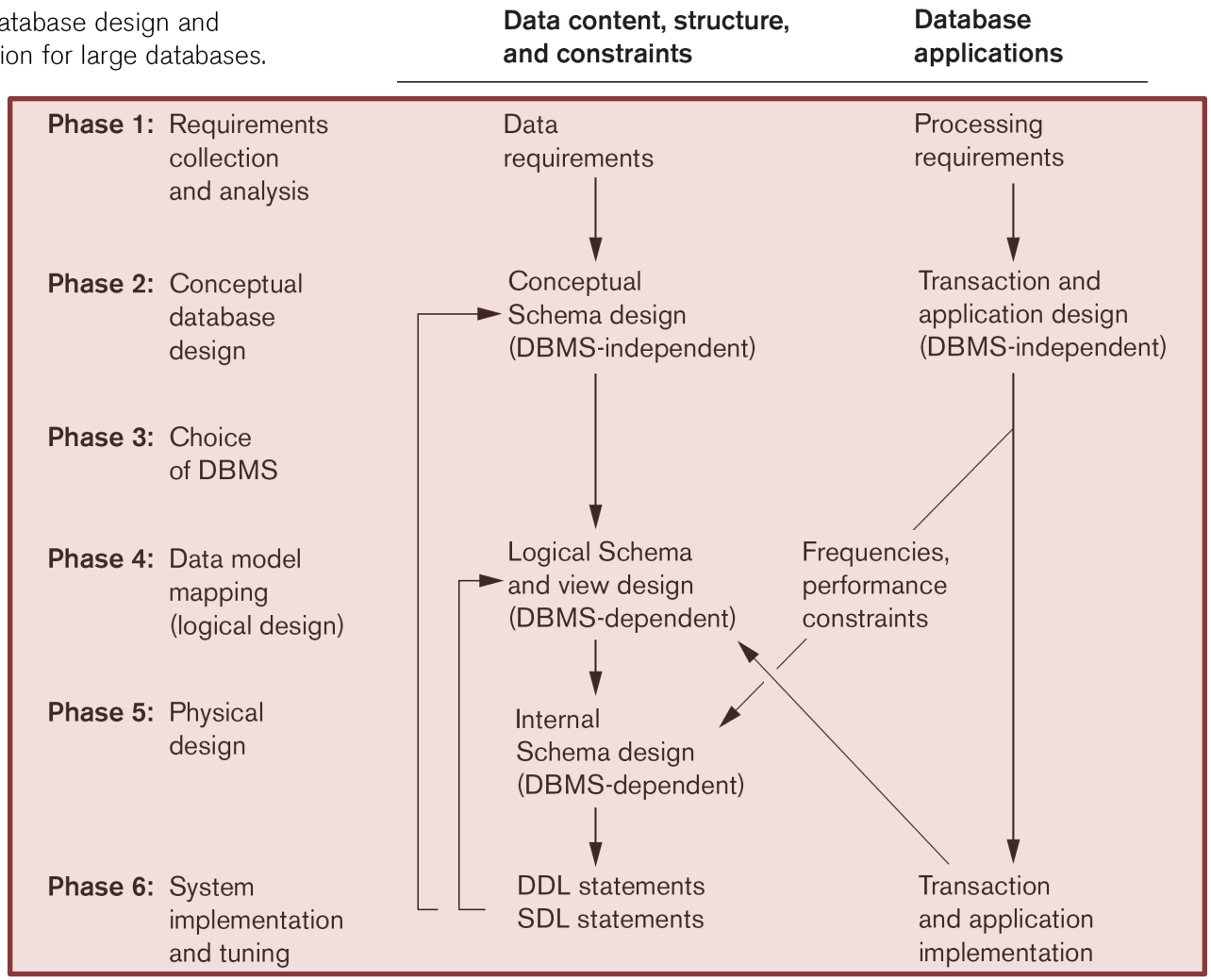


Outline

- Context
- Access Control
  - Strong password policies, 2FA
  - Discretionary, Mandatory
  - Least Privilege, Separate Privileges
- Attacks
  - SQL Injection
  - DoS (limit password length!)
  - Brute force password attempts (iCloud)
  - Internal vs. External (80% internal via Oracle)
  - Separate server, updates, audit logs
- Inference Control
- Encryption
  - Symmetric, Asymmetric, Hashing – tricky to get right!
  - Whole Database (and backups!), Communication
  - Sensitive Data (salting)

Database Design and Implementation Process

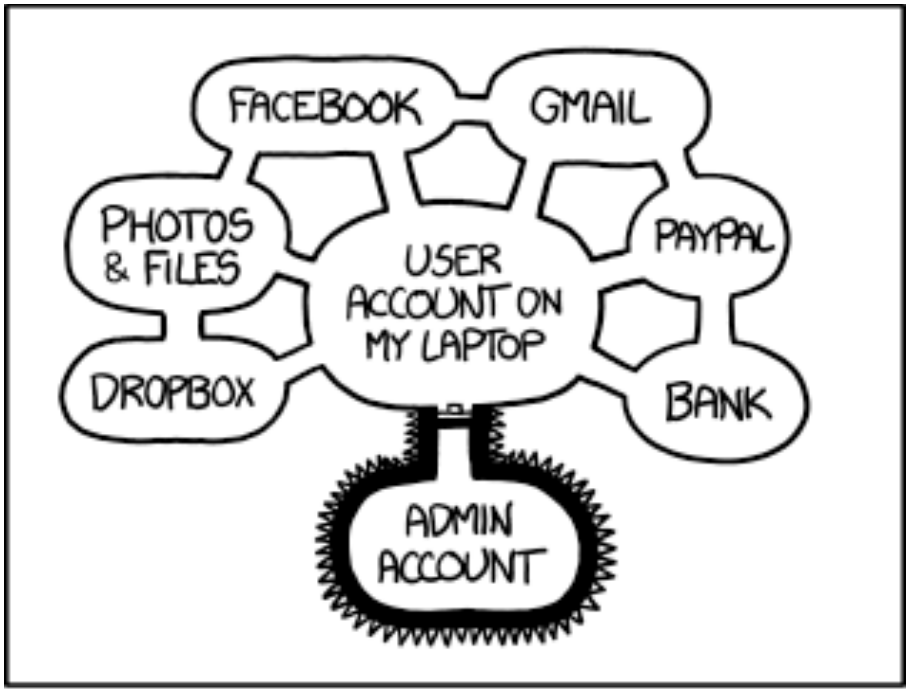
Figure 10.1
Phases of database design and implementation for large databases.



Guidelines

- Security as first-class citizen
  - *Early on security was an add-on, now it is everything*
- Security via depth
  - *Don't assume a firewall will save you*
- Design for failure
  - *What happens after a breach occurs?*
- Secure the weakest link
  - *Anything but the crypto!*
- Obscurity is not security
  - *Keys in binary stand out like sore thumbs*
  - *Stored procedures are not a cure for access control*

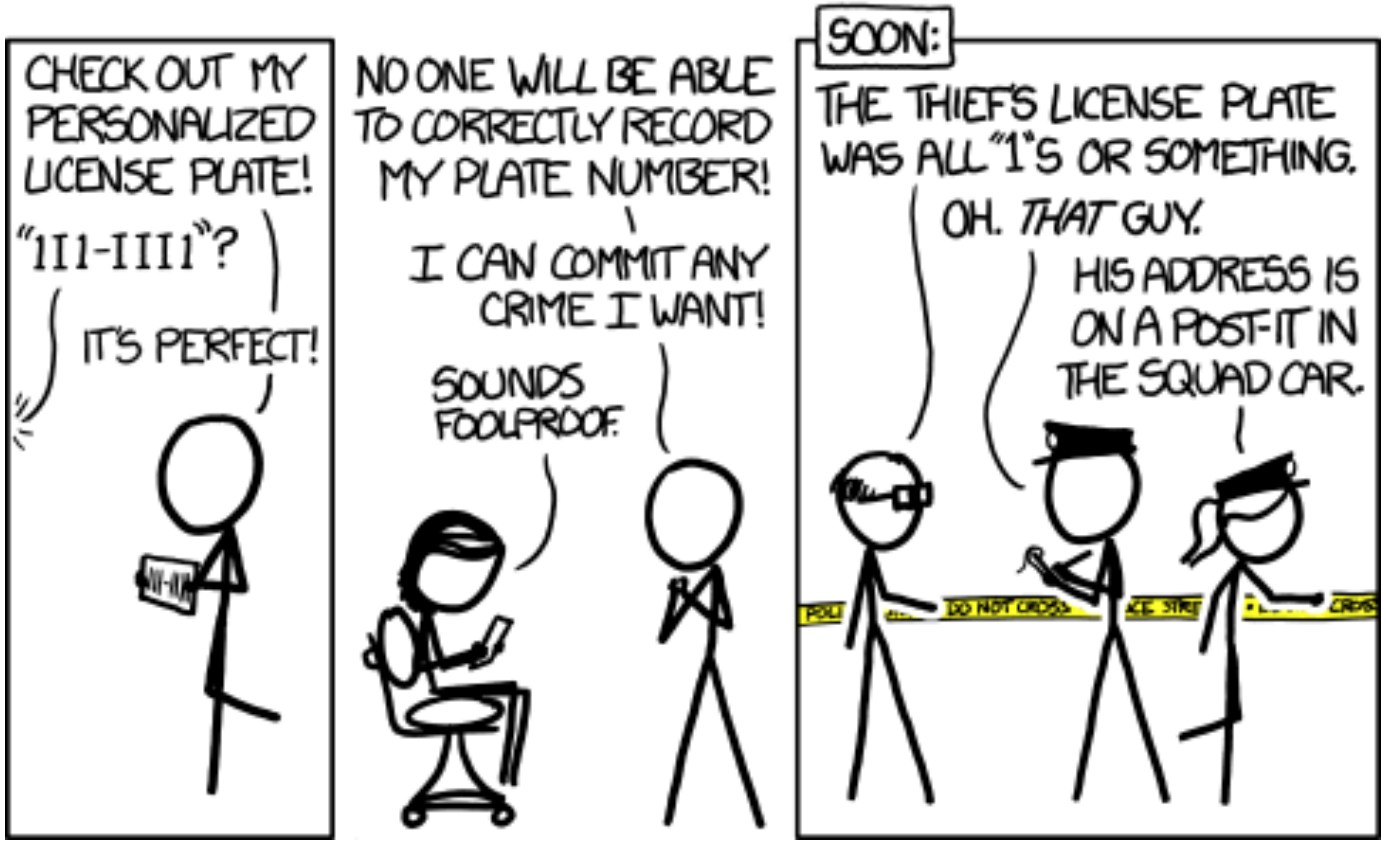
XKCD: Authorization



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

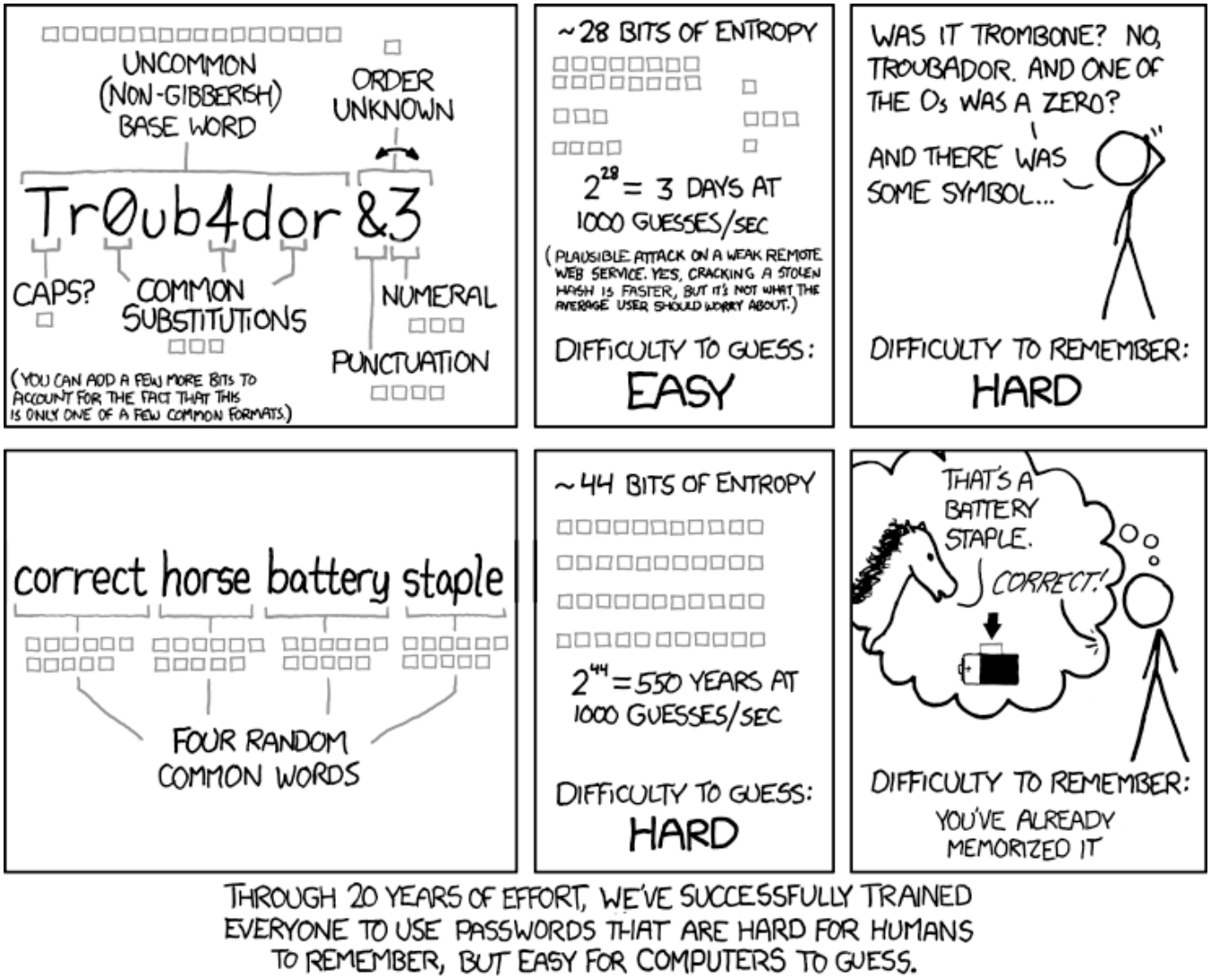
XCKD: License Plate



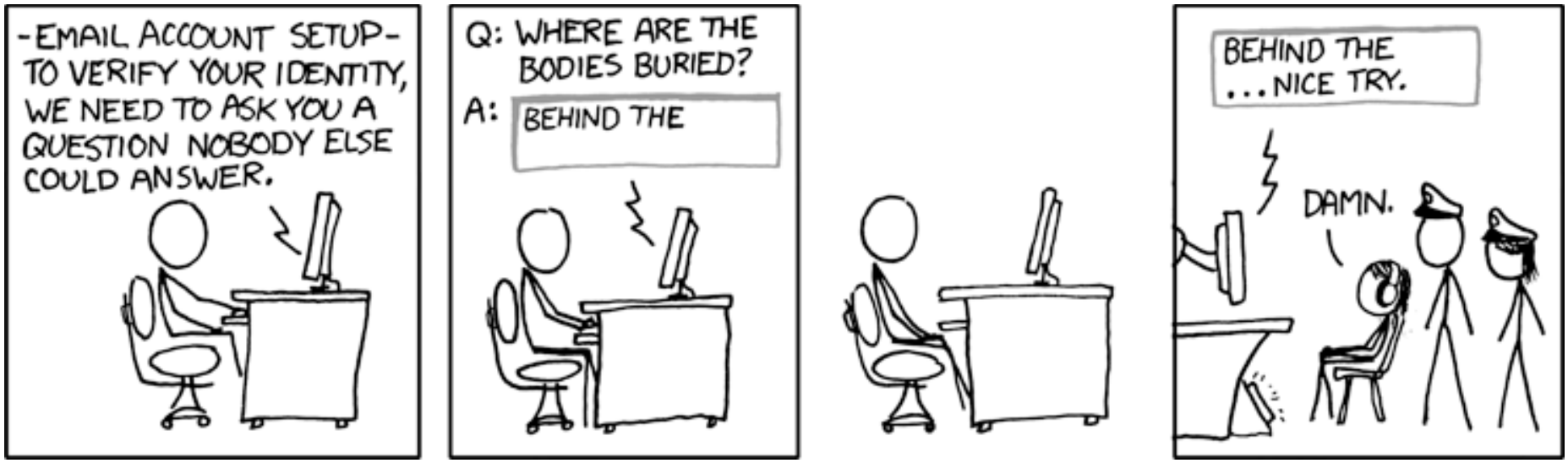
Authentication Policies

- Passwords
  - Enforce minimum length/complexity
    - Also maximum (more later w.r.t. DoS)
  - Require updates
  - Goal: make guessing/cracking difficult
    - Cross-service
- Attempts
  - Enforce limits to avoid brute force (iCloud)
- 2 Factor Authentication (2FA)
  - Often infeasible
  - Implementation may weaken
    - e.g. Social engineering

XKCD: Password Strength



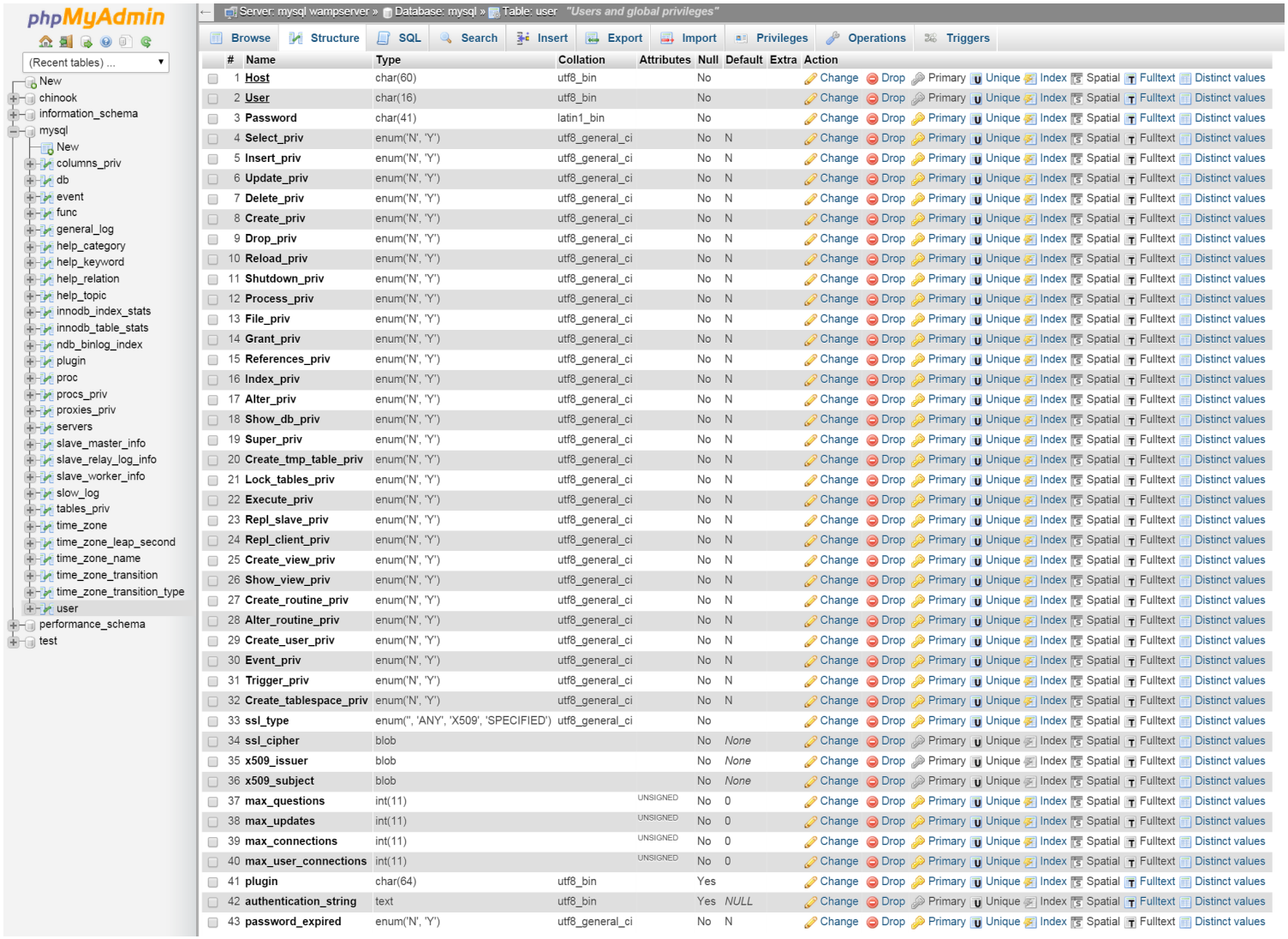
XKCD: Security Question



Discretionary Access Control

- Users **grant/revoke** privileges to other users
  - Starts with root/superuser/dba
  - with **`GRANT OPTION`**
- Privileges typically apply at multiple levels
  - Global, database, table, column
- Access matrix model
  - Users x Objects
- Fairly universal

MySQL (user)



#	Name	Type	Collation	Attributes	Null	Default	Extra	Action
1	Host	char(60)	utf8_bin		No			Change Drop Primary Unique Index Spatial Fulltext Distinct values
2	User	char(16)	utf8_bin		No			Change Drop Primary Unique Index Spatial Fulltext Distinct values
3	Password	char(41)	latin1_bin		No			Change Drop Primary Unique Index Spatial Fulltext Distinct values
4	Select_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
5	Insert_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
6	Update_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
7	Delete_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
8	Create_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
9	Drop_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
10	Reload_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
11	Shutdown_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
12	Process_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
13	File_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
14	Grant_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
15	References_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
16	Index_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
17	Alter_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
18	Show_db_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
19	Super_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
20	Create_tmp_table_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
21	Lock_tables_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
22	Execute_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
23	Repl_slave_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
24	Repl_client_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
25	Create_view_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
26	Show_view_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
27	Create_routine_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
28	Alter_routine_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
29	Create_user_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
30	Event_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
31	Trigger_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
32	Create_tablespace_priv	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values
33	ssl_type	enum('', 'ANY', 'X509', 'SPECIFIED')	utf8_general_ci		No			Change Drop Primary Unique Index Spatial Fulltext Distinct values
34	ssl_cipher	blob			No	*None*		Change Drop Primary Unique Index Spatial Fulltext Distinct values
35	x509_issuer	blob			No	*None*		Change Drop Primary Unique Index Spatial Fulltext Distinct values
36	x509_subject	blob			No	*None*		Change Drop Primary Unique Index Spatial Fulltext Distinct values
37	max_questions	int(11)		UNSIGNED	No	0		Change Drop Primary Unique Index Spatial Fulltext Distinct values
38	max_updates	int(11)		UNSIGNED	No	0		Change Drop Primary Unique Index Spatial Fulltext Distinct values
39	max_connections	int(11)		UNSIGNED	No	0		Change Drop Primary Unique Index Spatial Fulltext Distinct values
40	max_user_connections	int(11)		UNSIGNED	No	0		Change Drop Primary Unique Index Spatial Fulltext Distinct values
41	plugin	char(64)	utf8_bin		Yes			Change Drop Primary Unique Index Spatial Fulltext Distinct values
42	authentication_string	text	utf8_bin		Yes	*NULL*		Change Drop Primary Unique Index Spatial Fulltext Distinct values
43	password_expired	enum('N', 'Y')	utf8_general_ci		No	N		Change Drop Primary Unique Index Spatial Fulltext Distinct values

MySQL (db)

Server: mysql wampserver » Database: mysql » Table: db *"Database privileges"*

Browse | Structure | SQL | Search | Insert | Export

#	Name	Type	Collation	Attributes	Null	Default	Extr
1	Host	char(60)	utf8_bin		No		
2	Db	char(64)	utf8_bin		No		
3	User	char(16)	utf8_bin		No		
4	Select_priv	enum('N', 'Y')	utf8_general_ci		No	N	
5	Insert_priv	enum('N', 'Y')	utf8_general_ci		No	N	
6	Update_priv	enum('N', 'Y')	utf8_general_ci		No	N	
7	Delete_priv	enum('N', 'Y')	utf8_general_ci		No	N	
8	Create_priv	enum('N', 'Y')	utf8_general_ci		No	N	
9	Drop_priv	enum('N', 'Y')	utf8_general_ci		No	N	
10	Grant_priv	enum('N', 'Y')	utf8_general_ci		No	N	
11	References_priv	enum('N', 'Y')	utf8_general_ci		No	N	
12	Index_priv	enum('N', 'Y')	utf8_general_ci		No	N	
13	Alter_priv	enum('N', 'Y')	utf8_general_ci		No	N	
14	Create_tmp_table_priv	enum('N', 'Y')	utf8_general_ci		No	N	
15	Lock_tables_priv	enum('N', 'Y')	utf8_general_ci		No	N	
16	Create_view_priv	enum('N', 'Y')	utf8_general_ci		No	N	
17	Show_view_priv	enum('N', 'Y')	utf8_general_ci		No	N	
18	Create_routine_priv	enum('N', 'Y')	utf8_general_ci		No	N	
19	Alter_routine_priv	enum('N', 'Y')	utf8_general_ci		No	N	
20	Execute_priv	enum('N', 'Y')	utf8_general_ci		No	N	
21	Event_priv	enum('N', 'Y')	utf8_general_ci		No	N	
22	Trigger_priv	enum('N', 'Y')	utf8_general_ci		No	N	

MySQL (tables_priv)

Server: mysql wampserver » Database: mysql » Table: tables_priv *"Table privileges"*

Browse | Structure | SQL | Search | Insert | Export | Import | Privileges | Operations | Triggers

#	Name	Type	Collation	Attributes	Null	Default	Extra
1	Host	char(60)	utf8_bin		No		
2	Db	char(64)	utf8_bin		No		
3	User	char(16)	utf8_bin		No		
4	Table_name	char(64)	utf8_bin		No		
5	Grantor	char(77)	utf8_bin		No		
6	Timestamp	timestamp		on update CURRENT_TIMESTAMP	No	CURRENT_TIMESTAMP	ON UPDATE CURRENT_TIMESTAMP
7	Table_priv	set('Select', 'Insert', 'Update', 'Delete', 'Creat	utf8_general_ci		No		
8	Column_priv	set('Select', 'Insert', 'Update', 'References')	utf8_general_ci		No		

MySQL (columns_priv)

Server: mysql wampserver » Database: mysql » Table: columns_priv *"Column privileges"*

Browse | Structure | SQL | Search | Insert | Export | Import | Privileges | Operations | Triggers

#	Name	Type	Collation	Attributes	Null	Default	Extra
1	Host	char(60)	utf8_bin		No		
2	Db	char(64)	utf8_bin		No		
3	User	char(16)	utf8_bin		No		
4	Table_name	char(64)	utf8_bin		No		
5	Column_name	char(64)	utf8_bin		No		
6	Timestamp	timestamp		on update CURRENT_TIMESTAMP	No	CURRENT_TIMESTAMP	ON UPDATE CURRENT_TIMESTA
7	Column_priv	set('Select', 'Insert', 'Update', 'References')	utf8_general_ci		No		

Mandatory Access Control

- Objects are classified with security levels
- Users are afforded security clearance
- Government model, not typically supported

Privilege Policies

- Principle of least privilege
- Privilege separation
  - Multiple users, each with least privilege
- Abuse
  - Unauthorized
    - Mitigate escalation attacks
  - Authorized
    - Teachers changing grades
    - Firing a DBA

SQL Injection

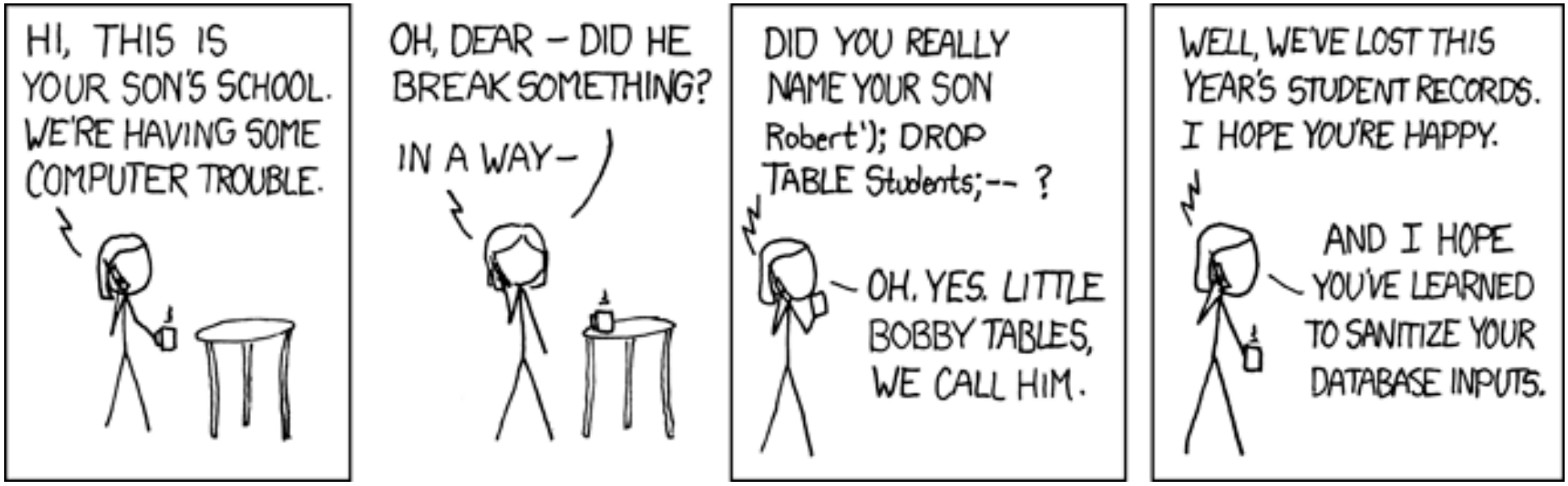
SQL manipulation for nefarious purpose

Method
- String manipulation
  - Parameters, function calls
- Code injection (e.g. buffer overflow)

Goals
- Fingerprinting
  - Learn about service via version, configuration
- DoS
- Bypass authentication/privilege escalation
- Remote execution

Protection
- Parameterized statements
- Filter input
- Limit use of custom functions

XKCD: Exploits of a Mom



Denial of Service (DoS)

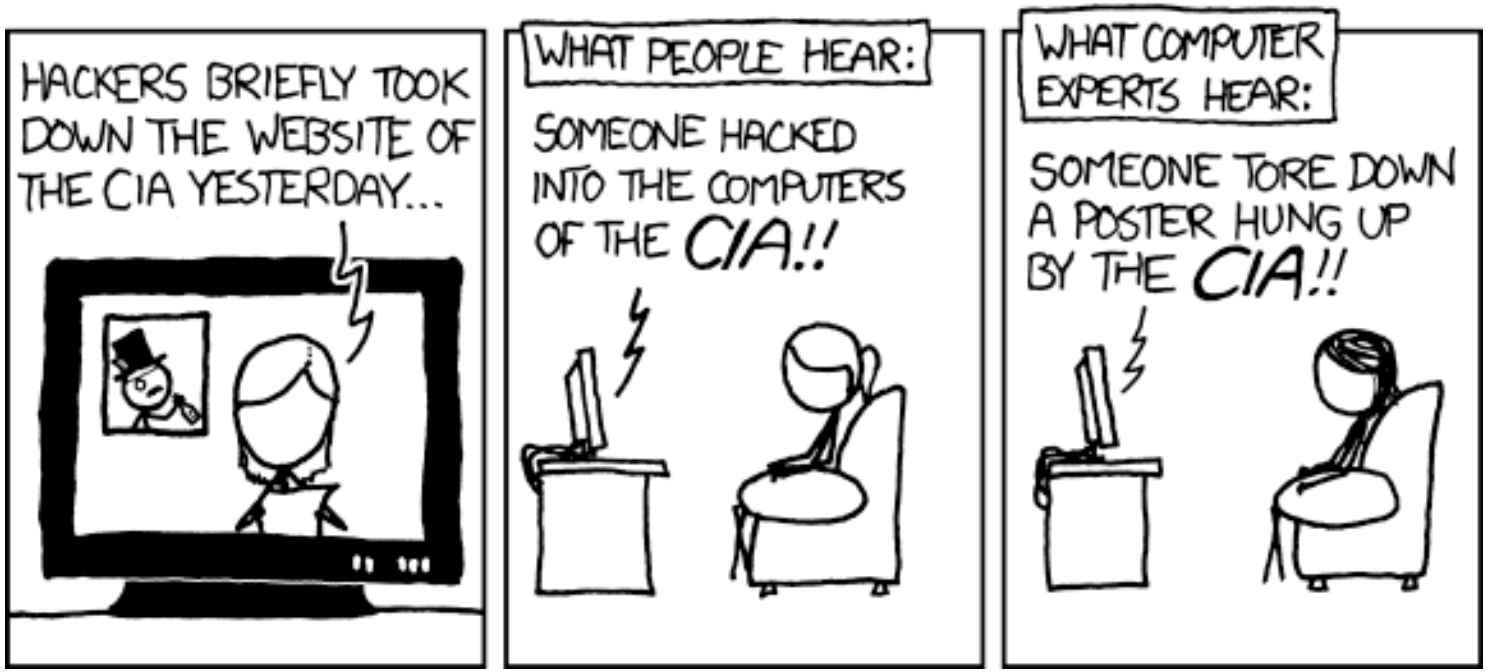
Any exposed interface

- Failed login
  - Lock out users
  - Resource utilization via long password verification
- Complex queries

Mitigation

- Resource limits
- Patching
- Monitoring

XCKD: CIA


HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

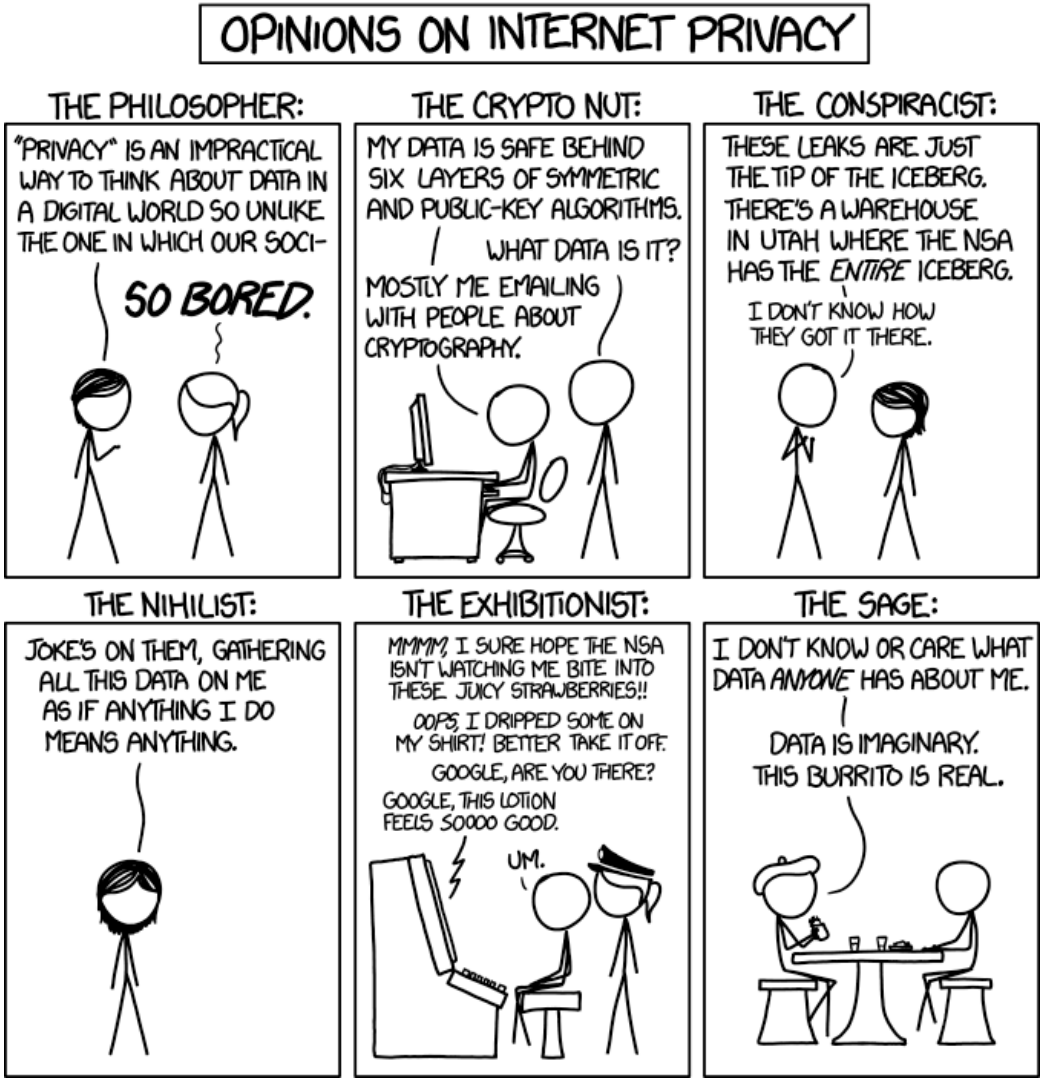
Protection

- Protect against internal attacks
  - Oracle: up to 80% of data loss
- Isolate DBMS
  - Separate machine, VM
- Regular patching policies
- Audit logs

Inferential Security

- Relevant when offering parameterized access to aggregate data
  - But must protect sensitive individual data!
- Prior knowledge and/or clever exploration might yield queries that reveal private information
  - Find “average” salary of <insert conditions that identify single individual>
- Techniques
  - Minimum result set size threshold
  - Added noise
  - Group partitioning

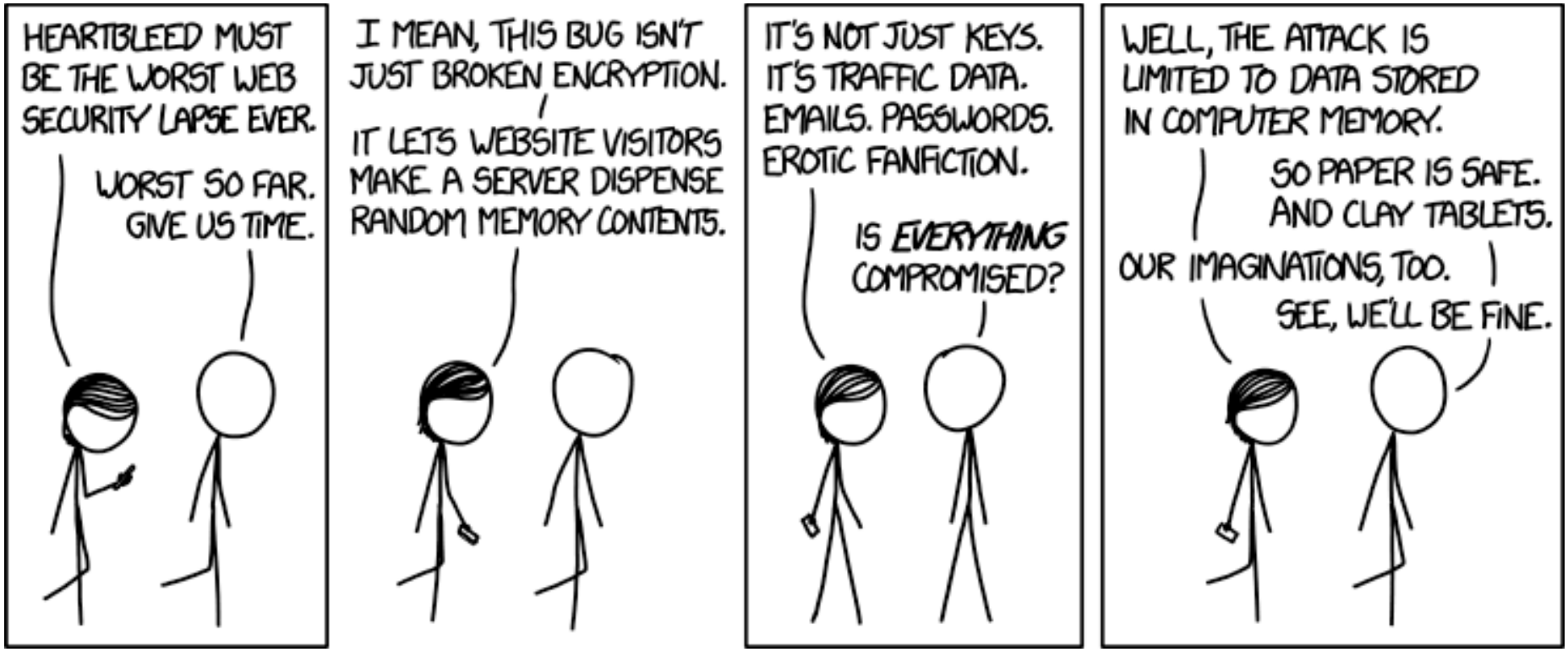
XKCD: Privacy Opinions



Encryption

- Symmetric
  - Single key encrypts/decrypts
- Asymmetric
  - 2 Keys: public encryption, private decryption
- Hashing
  - No decryption
- Encryption theory is solid, implementation is tricky
  - High-quality randomness
  - Bug-free code

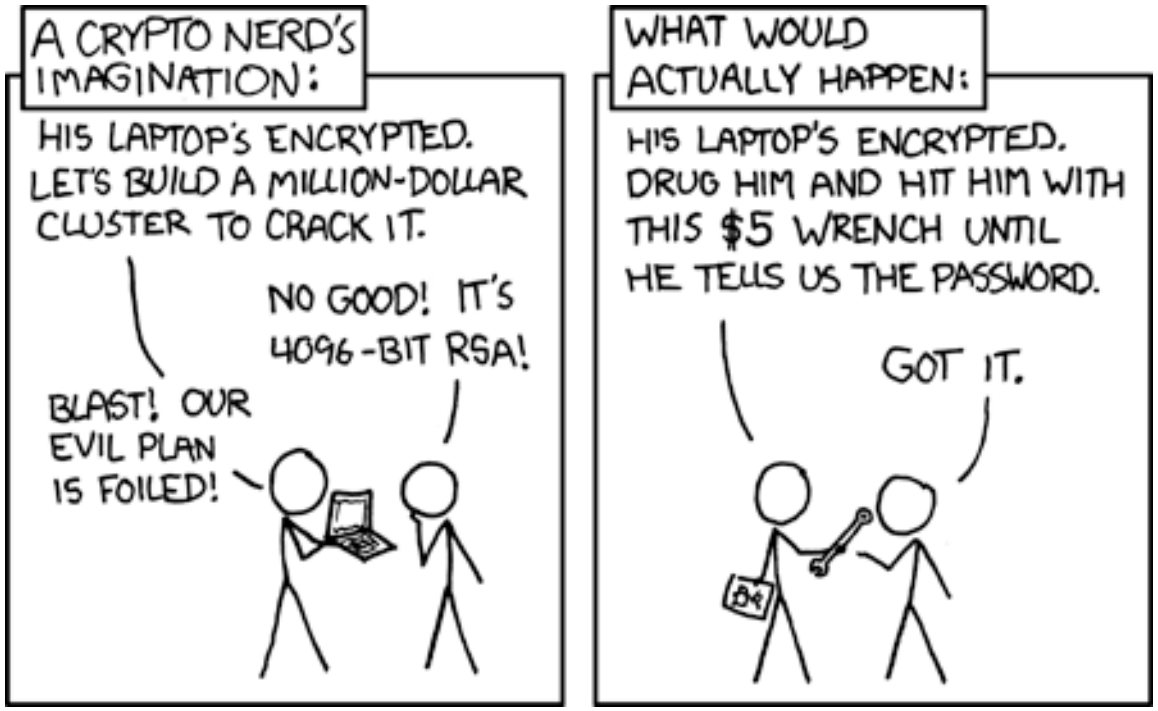
XCKD: Heartbleed



Basics

- Encrypt database files
  - Including backups!
  - Native or 3rd-party wrapper
  - Can be difficult to implement while being resilient to restarts, high-performance
- Encrypt application communication

XCKD: Security



Sensitive Data

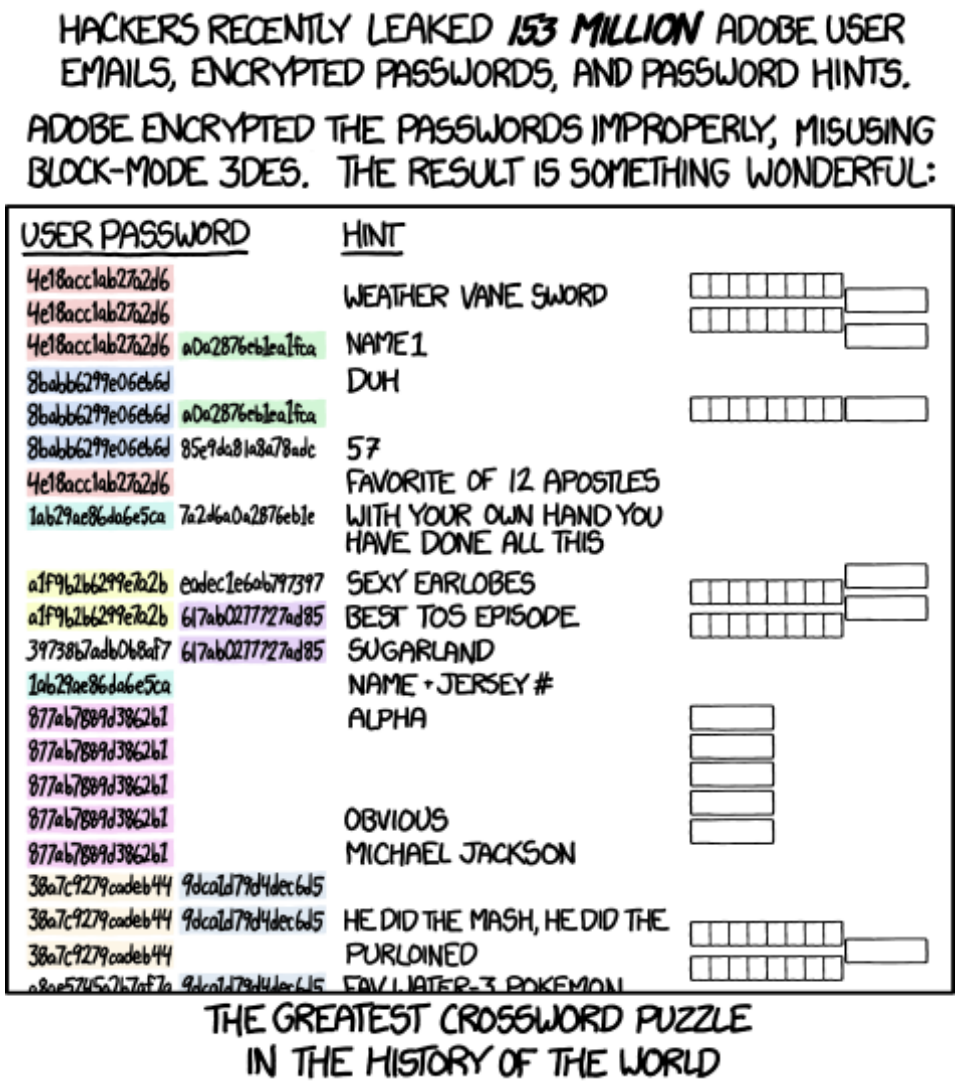
- When dealing with sensitive data, always consider how it needs to be used
- If only verification (e.g. password), hash
- If usage, encrypt
  - Ideally segment usage (e.g. CC entry vs. processing = public/private + last 4 as string)

Password Salting

- Salt = additional input prepended to hashed value
  - Ideally 1 salt per sensitive value
  - Stored text = salt, hash(salt + sensitive value)
    - Possibly several hashes

- Increases complexity of usefully processing bulk data
  - Re-use within service, across services
  - Rainbow tables

XCKD: Encryptic



Summary

- When dealing with database applications, security needs to be a first-class citizen, considered at all levels, preparing for failure (the weakest link!)
  - Obscurity ≠ Security
- We covered issues/best practices related to authentication/authorization, common attacks, inference control, and encryption

XKCD: Password Reuse