Disclaimers

Informational Purposes:
This presentation is for informational purposes only and provided "as-is." The views expressed are those of the presenter(s) and may not represent our companies or organizations.

Accuracy:
While we strive for accuracy, we are not responsible for any errors or omissions.

Forward-Looking Statements:
Any forward-looking statements are based on current expectations and may differ from actual results.

Third-Party Information:
References to third-party information do not imply endorsement or guarantee of accuracy.

No Advice:
This presentation is not legal, financial, or professional advice. Consult your own advisors for specific advice.

Use of Information:
Use the information at your own risk. We are not liable for any damages from its use.

EDA CLINICAL

BACK TO THE FUTURE OF CLINICAL TRIALS: ZERO KNOWLEDGE PROOFS

James Joseph
CEO Statistician
EDA CLINICAL

Akbar Khamidov
Software Engineer
Phosphorus Cybersecurity

18JUL2024

EDA CLINICAL

Clinical Research 1.0 to 4.0

Version	Technologies	Data Management	Features	Challenges
1.0	Handwritten records, Paper case report forms	Manual record-keeping and early clinical trials	Controlled by physician clinical trials	Limited scalability, Data quality
2.0	Electronic Data Capture, Electronic case report forms	EDC Transition to electronic health records (EHRs)	Demographics, diagnoses, medications, lab orders	Data exchange standards, User adoption
3.0	Wearable devices, data standards	Data Lake Patient-centric, use of wearable devices	Biosample data, genetic info, social data, PROs, DDT	Data storage, Data integration
4.0	**Cloud, Digital Health Technologies, AI (Smartwatch, health tracker)**	**Monitoring multiple wearable devices using APIs**	**Real-time monitoring, extensive data collection for submission**	Privacy, Security, and Accessibility

EDA CLINICAL

Patient-Focused

- > "The methods described in this document can be used to **elicit what is important to patients**, which may in turn help inform understanding of disease/condition and clinical trial design. It may also help the generation and use of patient experience data, including clinical outcome assessments and patient preference information, to inform benefit-risk assessment"

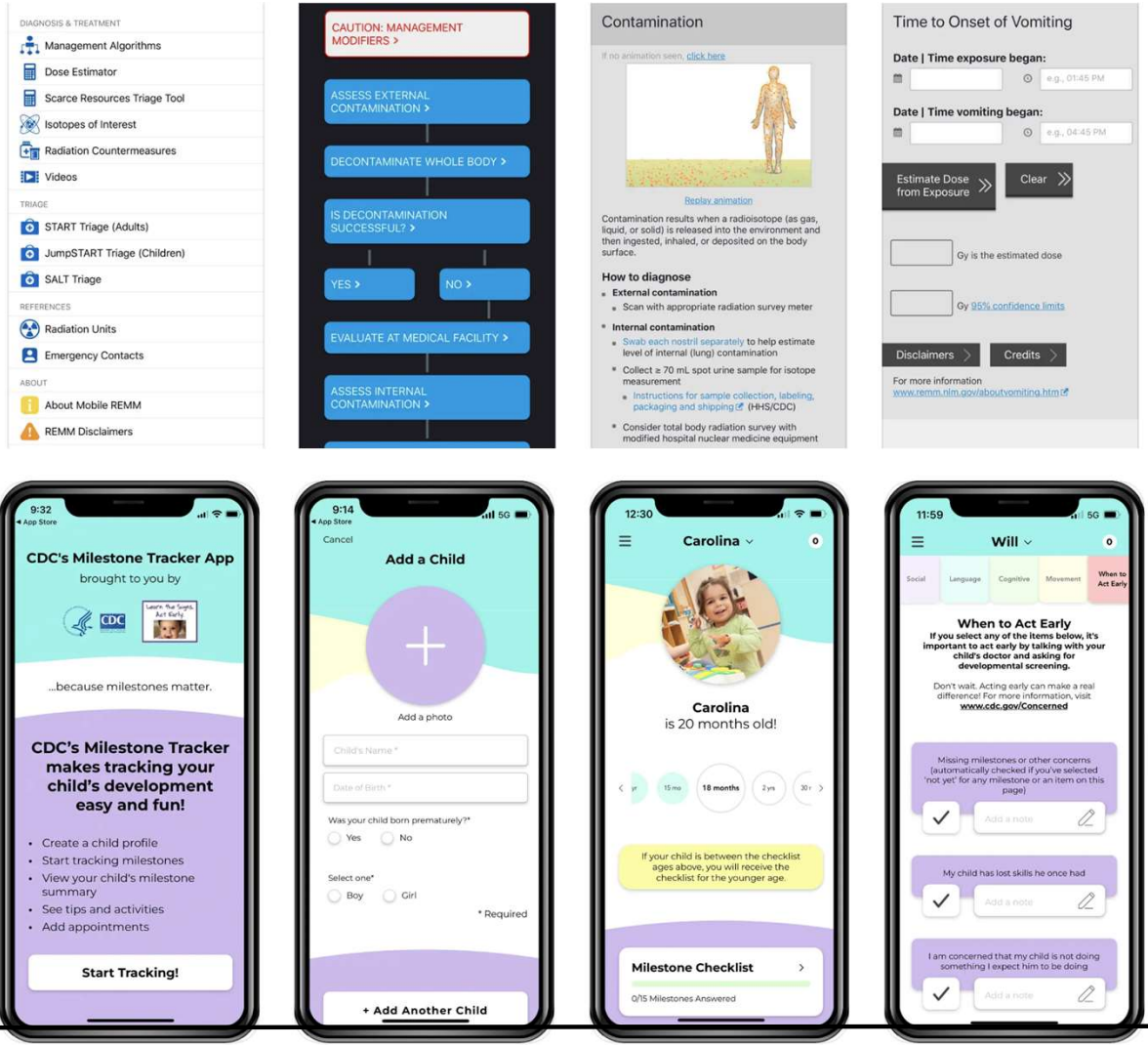
Patient-Focused Drug Development: Methods to Identify What Is Important to Patients Guidance for Industry, Food and Drug Administration Staff, and Other Stakeholders
February 2022
https://www.fda.gov/media/131230/download

EDA CLINICAL

Patient-Directed

- API task force
  - the **patient directed app** of API task force purview supports the patient's HIPAA right to access
- **CMS Stage 3 Objectives**:
  - Require healthcare providers to offer **patients electronic access to their health information** and to use health IT to **engage patients in their care.**
  - Encourage the use of APIs and other electronic means to facilitate patient access and data sharing.
  - Emphasize patient engagement and the coordination of care through interactive and interoperable health IT systems.

EDA CLINICAL



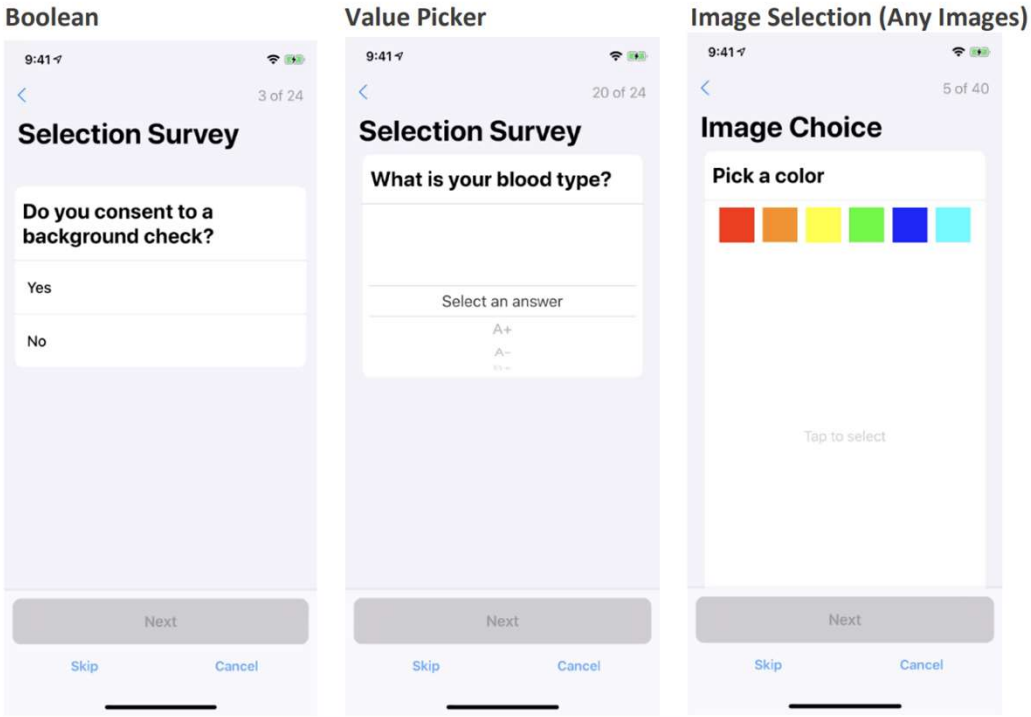
Mobile Medical Apps

- Software programs for smartphones and mobile devices
- Can be standalone, accessories, or a combination
- Examples: CDC Milestones Tracker, REMM app

EDA CLINICAL

FDA MyStudies App

- Background
- Benefits
- Roadmap

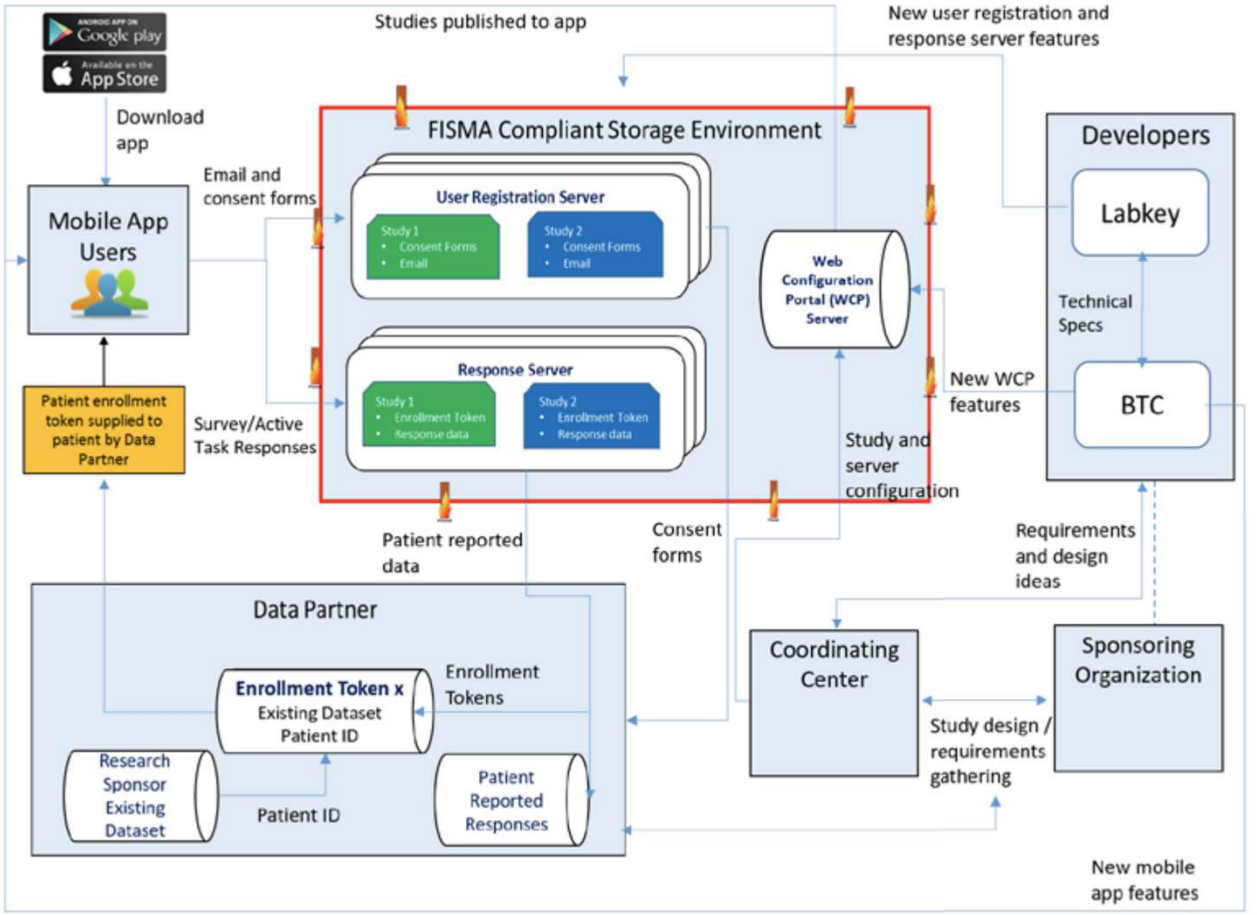


+ Single Select
Multi Select
Numeric
Time
Date
Open Text
Validated Email
Scale
Location
Mobile App Quick Overview for Research (fda.gov)

EDA CLINICAL

Secure Storage Environment

- FISMA complaint
- Partitioned for distributed research
- Responses can be downloaded in broadly compatible formats (e.g., for use in R, SAS, Excel, etc.)



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Federal Information Security Modernization Act (FISMA)

- § 3544(b)(1): "Periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of electronic information."
- § 3544(b)(2): "Policies and procedures that are based on risk assessments to ensure information security."
- § 3544(b)(3): "Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems."
- § 3544(b)(4): "Security awareness training to inform personnel of information security risks and responsibilities."
- § 3544(a)(2): Ensures that the agency head provides information security protections commensurate with the risk and magnitude of harm.
- § 3544(b)(5): "Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices."
- § 3544(b)(7): "Process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in the information security policies, procedures, and practices."
- § 3544(b)(8): "Procedures for detecting, reporting, and responding to security incidents."

EDA CLINICAL

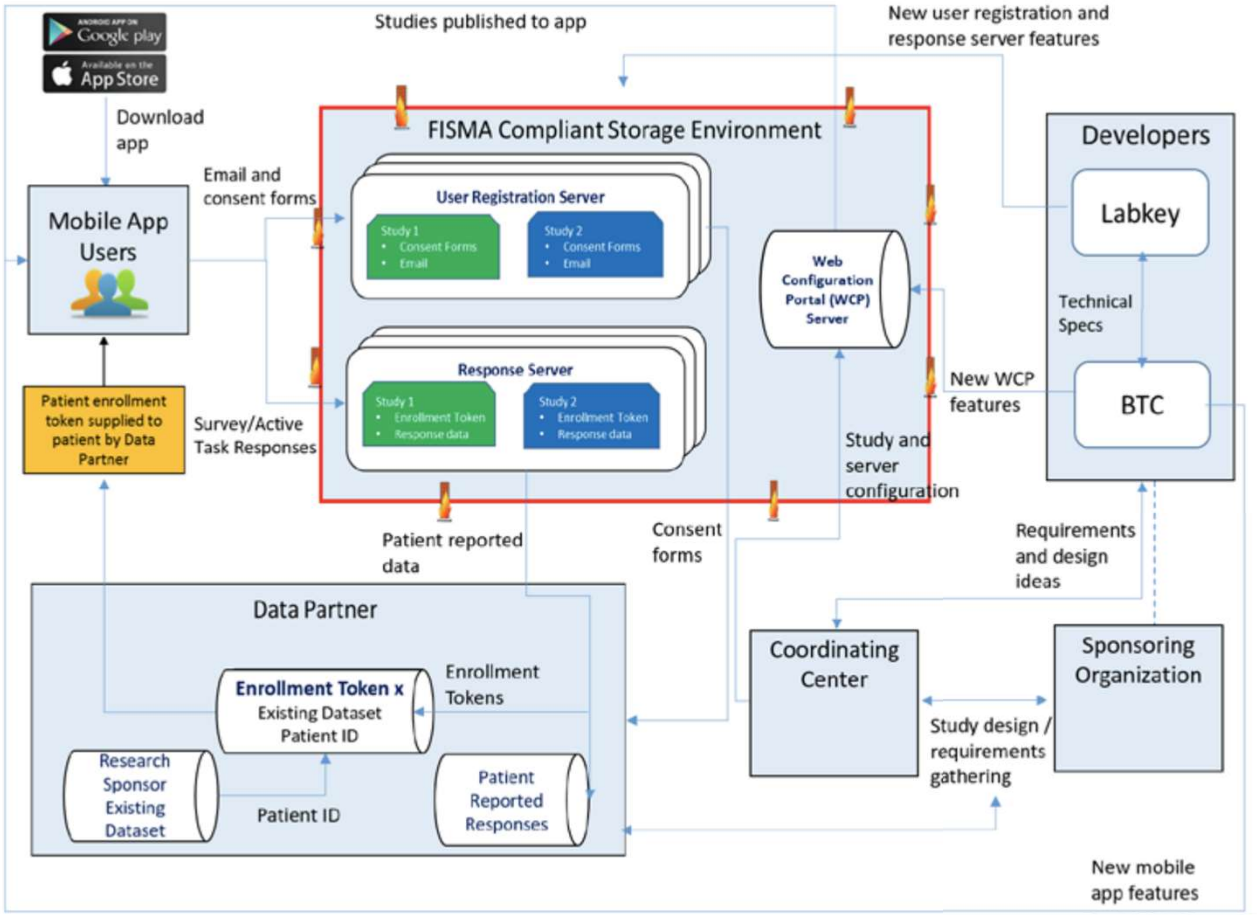
Common Attack Vectors for FISMA-Compliant Central Databases

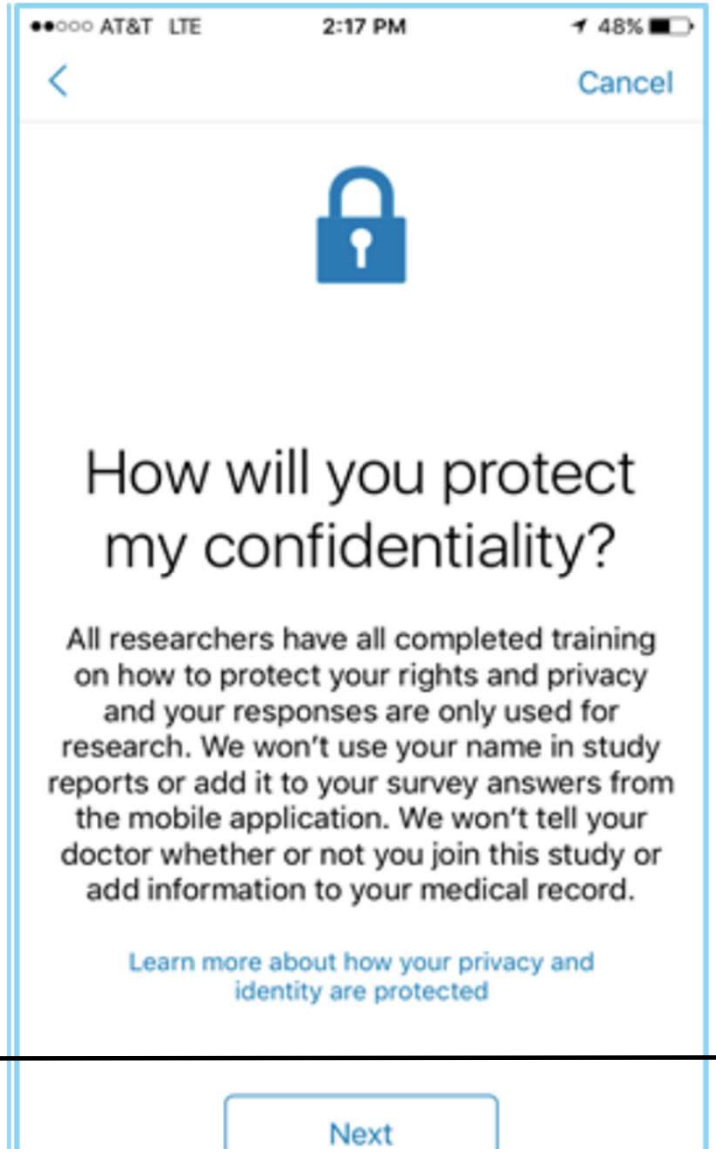
- Phishing and Social Engineering
- Insider Threats
- Misconfigured Security Settings

EDA CLINICAL

Secure Storage Environment

- FISMA complaint
- Partitioned for distributed research
- Responses can be downloaded in broadly compatible formats (e.g., for use in R, SAS, Excel, etc.)





EDA CLINICAL

Privacy addresses the question of who has access to personal information and under what conditions. Privacy is concerned with the collection, storage, and use of personal information, and examines whether data can be collected in the first place, as well as the justifications, if any, under which data collected for one purpose can be used for another (secondary)[2] purpose. An important issue in privacy analysis is whether the individual has authorized particular uses of his or her personal information (Westin, 1967).

Patient Data Privacy

- **Consent Fatigue**: This phenomenon occurs when individuals become overwhelmed or indifferent to consent requests, such as those for data collection or privacy policies, leading to less informed decision-making about their data.
- **Authentication Fatigue**: Need to trust our identity with the middleman.
- **Trust Issues**: WE have

EDA CLINICAL

API Task Force

- The **patient directed app** of task force purview supports the patient's HIPAA right to access his/her own PHI from a Covered Entity, as required under HIPAA § 164.502.
  - Any process that presents a substantially greater burden to the patient for API access approval should be considered **Information Blocking**

EDA CLINICAL

A zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that something is true, **without revealing any information…**

"The knowledge complexity of interactive proof system" 1985

EDA CLINICAL

Common Terms in Zero-Knowledge Proofs (ZKP)

Prover: The party that wants to prove the validity of a statement without revealing the underlying information.

Verifier: The party that checks the validity of the proof without gaining any knowledge about the underlying information.

Zero-Knowledge: A property that ensures no additional information is leaked during the proof process.

Interactive Proof: A proof that requires **interaction** between the prover and the verifier.

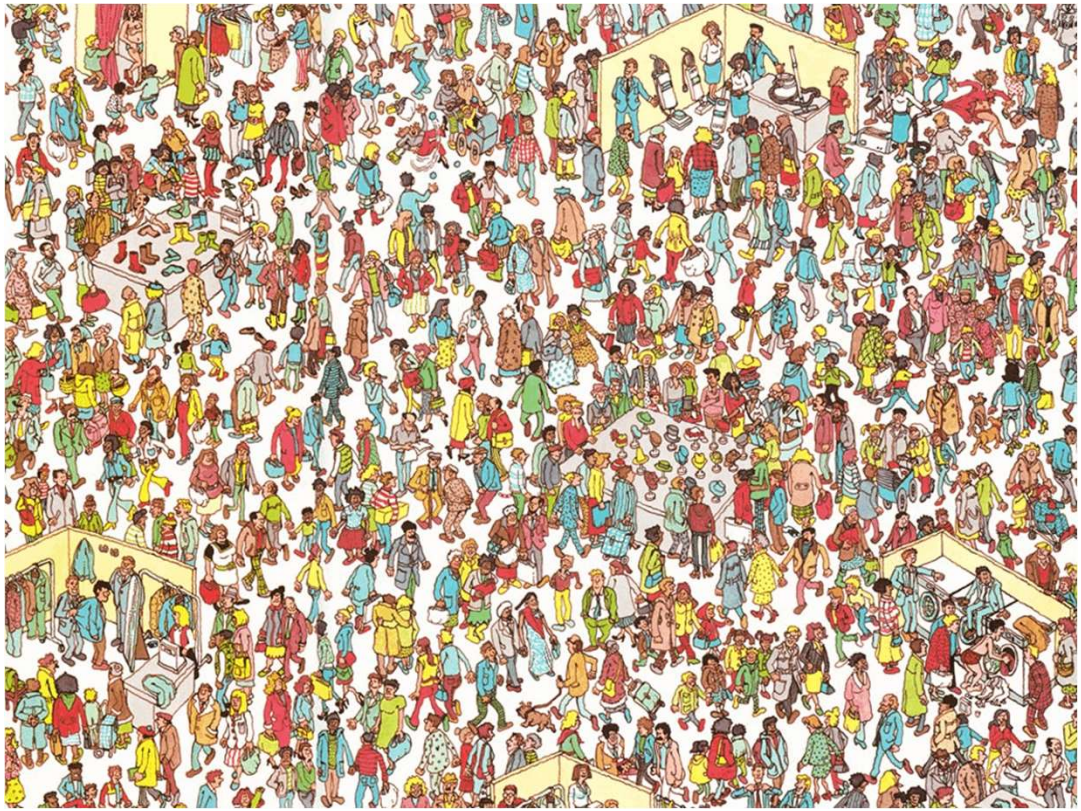
Completeness: If the statement is true, an honest verifier will be convinced by an honest prover.

Soundness: If the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability.

Proving Circuit: A computational representation of the problem to be proven, often used in ZKP schemes to structure the proof.

EDA CLINICAL

1: Non-interactive (deterministic) ZKP



EDA CLINICAL

2: Interactive (probabilistic) non-ZKP

Alice turns her back, Bob flips a coin and puts either Coke or Pepsi into a paper cup according the result

Alice tastes and announces whether she thinks it was Coke or Pepsi.

If they repeat this k times and Alice always answers correctly then Bob can conclude with $1 - 2^{-k}$ probability that she really can tell the difference.

lec15.pdf (princeton.edu)

EDA CLINICAL

3: Interactive (probabilistic) ZKP

Scenario:

- You have two billiard balls: one red, one green.
- Your color-blind friend can't distinguish them and is skeptical.

Objective:

- Prove the balls are differently colored without revealing which is red or green.

Proof System:

- Friend holds one ball in each hand.
- He puts his hands behind his back and either switches the balls or not (50/50 chance).
- He brings his hands out, and you "guess" if he switched the balls.

EDA CLINICAL

Key Points Interactive ZKP

Identifying Switches:

- You can accurately guess if the balls were switched by their colors.
- If the balls were identical in color, you could only guess correctly 50% of the time.

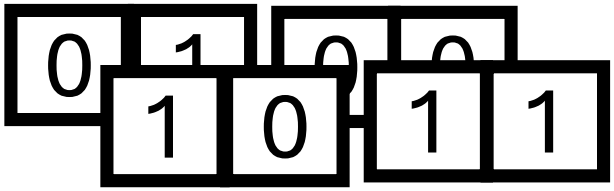
Repetition for Conviction:

- Repeat the process ttt times (large ttt).
- If you guess correctly every time, your friend is convinced the balls are different.
- Probability of guessing correctly all times if balls were same color: 2^{-t}.

Zero-Knowledge:

- Friend never learns which ball is red or green.
- He gains no knowledge about distinguishing the balls' colors.

EDA CLINICAL



James (Verifier) does not know bits <u>are different.</u>

Verifier Can	Prover States	Verifier's Confidence
Switch	N/A	?
Switch	Switch	+1%
Switch	No Switch	-100%
No Switch	N/A	?
No Switch	No Switch	+1%
No Switch	Switch	-100%

∞

James does not know bits <u>are not different</u>.

Verifier Can	Prover States	Verifier's Confidence
Switch	N/A	+1%
Switch	Switch	?
Switch	No Switch	-100%
No Switch	N/A	+1%
No Switch	No Switch	?
No Switch	Switch	-100%

∞

EDA CLINICAL