Avoiding Bias in Implementations of Randomized Protocols in Security Screening

Fred S. Roberts
Security Screening at Large Gathering Places

• As events in recent years have demonstrated, any place where many people gather is a target for terrorists and others who intend harm.

• Places of concern include:
  – Airports
  – Train Stations
  – Sports Stadiums
  – Concert Halls/Theatres
  – Casinos
  – Convention Centers
  – Malls
The Problem

• The November 2015 terrorist attacks in Paris at the Stade de France, the Bataclan, and restaurants and bars highlighted the need for security at large gathering places.

Credit: commons.wikimedia.org
Credit: En.wikipedia.org
The Problem

• So did the May 2017 attack at an Ariana Grande concert at the Manchester Arena.
• And the October 2017 attack at a country music concert in Las Vegas.

Manchester arena after attack
Credit: en.wikipedia.org
BBC picture

Las Vegas 2017
Credit: timesofisrael.com
The Problem

- The public areas of airports were attacked in Brussels, Istanbul, Ft. Lauderdale.

After Brussels Airport bombing, 2016
Credit: En.wikipedia.org

Istanbul Airport, bombed 2016
Credit: En.wikipedia.org

Fort Lauderdale airport shooting, 2017
Credit: sun-sentinel.com
Security Screening at Large Gathering Places

• Sports and entertainment venues (stadiums, arenas, etc.) host millions of patrons annually, form the basis for a multi-billion dollar industry, and present an inviting target for terrorists.

• In the U.S., in 2011, the National Football League (NFL) asked all of its stadiums to screen 100% of the patrons with hand-held metal-detecting wands.

Rutgers Stadium Credit: commons.wikimedia.org
Our Data Collection

• We worked with an NFL stadium to study the process.
• Data were collected using Observation and Video Analysis
• Initial Observation on site at football games in 2011 plus four 2012 events:
  – International Soccer – Mexico vs. Wales
  – International Soccer: Argentina vs. Brazil
  – Hot 97 Summer Jam
  – Advance Auto Parts Monster Jam
• Video analysis from football event
• Required new Java application to facilitate the recording of inspection times from video provided by partner stadium.
Data Analysis - SUMMARY

We evaluated the effect of several important factors on the inspection times:

- **Inspection method** (pat-down, wanding, or bag check)
- **Location** (gate, pod, lane ~ inspector)
- **Time before event** (early wave vs. late wave)
  - Early wave = from time of gate opening until waiting line is cleared
  - Late wave = from time of crowd accumulation until event start
- **Type of event/crowd demographics**
  (soccer match, monster truck)
Data Analysis

CONCLUSIONS

• Inspection time distributions differ significantly according to:
  ✓ Inspection methods
  ✓ Gates
  ✓ Times
  ✓ Events
  ✓ Inspectors

• Statistical analysis shows that the differences are much greater than can be explained by random chance.
Security Screening at Large Gathering Places

• Screening at sports and entertainment venues must be done in the context of a tradeoff between safety and patron satisfaction.

• Screening everyone with hand-held wands didn’t work: As the beginning of the event got close, and the security lines were long, management worried that patrons wouldn’t get in on time.

• So, they stopped using wands at some point and instead turned to “pat-downs.”
Security Screening at Large Gathering Places

• An alternative to get people into the stadium in time might have been to use some random procedure to inspect some of the patrons but not others.
• But it turned out that people objected to not having 100% screening. They wanted safety.
Security Screening at Large Gathering Places

- Walkthrough metal detectors (WTMDs) have some advantages over wands:
  - They allow faster throughput
  - They seem to be more accurate in catching contraband
  - Screeners don’t get tired from the bending required to wand people by hand.
- Soon, the National Football League required 100% use of WTMDs.
- The National Basketball Association, National Hockey League, etc., followed.
- Those who set off the alarm in a WTMD were subjected to secondary screening with wands.
CCICADA Stadium Simulator

- Developed to simulate patron screening processes when partner stadium investigated WTMD Issues:
  - How many WTMDs needed?
  - How many screeners needed?
  - What is the “throughput”?
  - Performance in bad weather?
  - Training

- Observed experimental WTMD use at partner stadium in December 2012.

- **Preliminary conclusion:** Small # of WTMDs unlikely to get everyone through quickly enough.
CCICADA Stadium Simulator

- The simulator is a patron screening tool that can consider
  - Variety of inspection methods
  - Know for each the “throughput,” the arrival rates at different times, the error rates, etc.
  - Have goals such as:
    - Getting everyone in by certain time
    - Not letting queues get too long – this produces vulnerabilities (and patron dissatisfaction)
    - Keeping maximum wait time low
  - Can you model which inspection process to use when and for how long?
Using CCICADA’s Stadium Simulator

• The parameters inputted into the model:
  – Arrival rates (which could differ for each game)
  – Number of lanes
  – Distribution of wanding times (these and other times could depend on type of clothing worn, e.g., function of weather)
  – Distribution of pat-down times
  – Distribution of WTMD times
  – Number of patrons in line before switching screening processes

• Model allows you to use any numbers that make sense for a given arena. (Or use numbers based on our observations.)

• The user can specify which screening method (or combination of methods) to use.
Stadium Simulator Output

• The simulator output file includes the following; each can be used to make decisions about screening policy:
  – Total arrivals
  – Total arrivals at event start (kick-off)
  – Max number of patrons in line
  – Number of patrons in line at kick-off
  – Queue “clearance” time (time last person entering before kick-off is in)
  – Screening switch time
  – Number of patrons inspected by each method
  – Max waiting time per patron

Those queues create a vulnerability.
Image credit: Phil Roeder, Creative Commons
CCICADA’s Stadium Simulator

Most of the parameters can be obtained by choosing a representative game

- **Parameters**
  - Arrival rates
  - Number of lanes
  - Wanding times
  - Pat-down times
  - WTMD times

- **Screening Strategy**
  - Switching inspection type (Y/N)
    - Number of patrons in queue to switch the process, or
    - Time of switch
  - Does phase 2 include randomization? (Y/N)
    - Ratio of patrons in each type of inspection in the randomization

The model output file includes

- In Queue @ kickoff
- Queue clearance time
- Max Waiting Time per patron
- Max queue length
CCICADA’s Stadium Simulator

• The simulation tool can be tuned for use at different venues and has been developed with input from various venues.

• The model can help answer many questions. For example:
  – How many WTMDs would be needed to ensure the queue clears by 5 minutes after event time?
  – If we have 60 lanes of wanding at a gate, how long will the queue get?
  – If we switch from wanding to pat-downs when the lines get too long, what should the length be in order to get everyone in by 5 minutes after event time?

• This helped the stadium decide on different screening protocols.
Then Came Paris 2015

• The November 2015 Paris attacks changed a lot.
• In the U.S., meetings were convened on how to increase security at large gathering places.
• Some of the discussion focused on randomization.
  – Not to use as a tool for less screening when you can’t screen everyone.
  – But as a tool to confuse an attacker and make an attack more risky.
Randomization: Outline

• We will explore the many ways to randomize in security at large sports and entertainment venues.
• In sports and entertainment venues, there is a tradeoff between enhanced security and patron satisfaction. Or is there?
• Implementation needs to be fair and unbiased. What does that mean?
• It can be perfectly fair and unbiased, yet patrons might feel that it is not – there are issues of perception of fairness.
• How one implements a randomization protocol affects its fairness and perception of fairness.
• How can you explore the effects of an implementation before you actually do it?
Goals of Randomization

- Primary goal: making it more complicated/confusing/expensive for adversaries, which acts as a deterrent.
- Monitoring operational integrity
  - E.g., by randomly rechecking credentials of employees
- Stimulating the capability or alertness of security personnel.
  - E.g., through use of red-teams or “secret shoppers”.
- Achieving intermediate levels of security when threat intelligence and/or budget considerations do not recommend 100% application.
  - E.g., when inspecting some fraction of persons or covering part of a venue with cameras is better than not doing anything.
The Many Faces of Randomization

- Randomization can be applied to:
  - The patrons
  - The security camera monitoring
  - The pre-event venue inspections
  - Access control for employees and patrons
  - Employee badge verification
  - Background checks on employees
  - The media
  - The loading dock
  - The parking area
  - …

- It should *not* be focused on only one part of the security profile.
Benefits of Randomization

• When a process is too expensive to do 100% of the time, randomization can still reduce threats and increase security. It is a low-cost way to introduce a higher level of security.
• There are advantages to being unpredictable.
• Randomization makes the “bad guys” work harder; it gives them pause for thought.
• Randomization diminishes the effectiveness of surveillance by the adversary. The goal is to defeat a sophisticated surveillance team.

Image credit: commons.wikimedia.org
Benefits of Randomization

• Randomization keeps those with intent to do harm off balance.
• Randomization serves as a deterrent: If procedures are seen to be uncertain, unpredictable, adversaries might alter their calculation of the likelihood of success or failure.
• Deterrence is especially effective when it is known that a random security process is being implemented, but the exact protocol or randomization scheme is not visible.

Image credit: commons.wikimedia.org
Secondary Screening

• Adding a randomized secondary check improves security in two ways
  – It raises the detection rate through catching more on a second try.
  – The visible additional security has some level of deterrent effect.
Randomization in Patron Screening

• There are many ways that venue security managers and collaborators can add randomization to patron screening processes, as well as in areas outside of the venue prior to patron screening.

• They can start at the parking lot or exit from the metro.

• They can add secondary screening at various steps.

Image credit: commons.wikimedia.org
The many ways in which randomization might be applied to patron screening
Randomization in Other Areas

• In addition to patron screening, randomization can be implemented in many other aspects of security:
  – Randomly choose where security cameras look
  – Randomly choose order of pre-event security “sweeps”
  – Randomly inspect employees in different ways
  – Randomly assign staff to jobs/locations they are trained for.
  – Randomly check or re-check vendor deliveries
  – Randomly check or re-check media
  – Randomly do background checks on employees

• There is need for algorithms in all of these areas.

credit: commons.wikimedia.org
What does it Mean to be Fair and Unbiased?

- A key principle is that implementation of randomization should be unbiased and fair.
- This means you should not discriminate against people in different groups.
- It means that a person in one group should have the same probability of being selected for a security procedure as a person in another group.
- However, that doesn’t mean you shouldn’t pick out people for extra screening if there are behavioral indications that you should.
  - E.g., heavy winter coat in summer.

Image credit: En.wikipedia.org
What does it Mean to be Fair and Unbiased?

• What does fairness mean?
• Simple version: you don’t get screened faster than anyone else, or get to move to the head of the line, or bypass screening.

Image credit: En.wikipedia.org
What does it Mean to be Fair and Unbiased?

• But even that may not be what you want.
• Many stadiums have different lines for people with bags and people without bags.
• That seems fair.
• What about children? Do they need the same scrutiny as adults?
  – An attacker could hide contraband on a child.
What does it Mean to be Fair and Unbiased?

• What does fairness mean?
• Fair allocation of resources literature is relevant.
• Resource could be “free passage without extra screening.”
• Fair allocation literature: how well individuals or groups are treated in relation to each other.
• Notions in the literature include*:
  – No-envy
  – Egalitarian-equivalence
  – Individual and collective lower & upper bounds on welfare
  – Notions of equal or equivalent opportunities
What does it Mean to be Fair and Unbiased?

• These notions from the literature on fair allocation are probably too sophisticated for the time being. Emphasis is on “simple” notions of fair – equal probability of selection.
• There is room for research on principles of fairness in screening.
• Doesn’t seem to be a literature on this topic.
How do you Avoid *Perceptions of Unfairness and Bias*?

- There is a considerable literature on perception of bias.
- We apply that to security screening.
- A serious concern in introducing randomization in patron screening is the possibility that patrons will see the selection process as biased or unfair.
- Being accused of “profiling” is a serious concern.

Credit: commons.wikimedia.org
Avoiding the Perception of Bias in Randomized Patron Screening

- Perceptions of biased treatment can be triggered or amplified in a number of ways.
- Understanding research on bias can be helpful.
- One view: Perceptions of bias are an estimation that there is a higher likelihood of events occurring because of an individual’s identification with a group than because of their individual characteristics, personality traits, or actions.

Credit: commons.wikimedia.org
Avoiding the Perception of Bias

- Perceptions of bias are an attribution of negative motives (selfish, egocentric) to others holding opposing viewpoints.
- These perceptions can be greatly influenced by situational context and individual motivations.
- When there is an expectation of stereotyping due to membership in a certain identity group, there is an individual’s perception of bias.

Credit: commons.wikimedia.org
Avoiding the Perception of Bias

• “Control” can be a mitigating factor in bias perceptions.
• Individuals care about fair procedures and just outcomes.
• When an individual experiences a loss of control, they are likely to use a “compensatory mechanism” like attribution of bias as a means of making sense of and reducing their distress.
• Any intervention that restores equilibrium to their sense of control will concurrently moderate their sense of being treated unfairly.
Recommendations to Avoid the Perception of Bias

- When there is a perceived alignment of values, there is a smaller likelihood of bias perceived.
- So, venues should have information available and distributed (via TV screens, pamphlets) reminding customers of value and importance of security protocols.
  - This appeals to their sense of/need for justice, fairness, safety, security, etc.

World War II US government security awareness poster
Credit: commons.wikimedia.org
Recommendations to Avoid the Perception of Bias

• Venues should positively reinforce the brand of the organization as being “fair” and “just.”
  – Notify the patrons that the organization seeks to protect and respect all customers.

• Keep patrons informed about and engaged in security protocol and procedures.
  – Prior to events, detail security protocols and procedures in marketing materials and, when possible, on tickets.
  – During events, use media and personnel to quickly and efficiently explain upcoming processes.
  – Obtain feedback from patrons about their experiences during security-related processes.
Recommendations to Avoid the Perception of Bias

• The expectation of stereotyping increases perceptions of bias.
• So organizations should seek to employ a perceivably diverse staff (race, ethnicity, gender, etc.).
• Staff should receive consistent diversity and de-escalation training.
  – Such training should be shaped directly from surveys of customer experiences with security enforcement.
  – The security staff should teach their employees that they must completely understand the importance of people’s civil rights.

Credit: commons.wikimedia.org
Recommendations to Avoid the Perception of Bias

• Implemented protocols should increase the customer’s sense of control during security enforcement processes.
  – A higher sense of control does not require that they have “real” control.
  – It does require that the process be easy to understand and be “predictably unpredictable.”
  – To accomplish the latter, selection for screening or additional screening should be transparent and visibly indifferent to individual characteristics.

• Note: *not all agree about transparency.*

• Some feel that you should not be too transparent as otherwise your protocol can be learned by an adversary.
Recommendations to Avoid the Perception of Bias

• Research challenge: which specific implementation procedures for randomization best fit these recommendations?

Credit: commons.wikimedia.org
Comments on Patron Satisfaction

• Patron satisfaction is dynamic.
• To date, increased security measures have on balance been viewed favorably.
• But venue managers do not know when additional processes will tilt patron satisfaction to the unfavorable side.
• This suggests regular monitoring of patron attitudes through surveys or social media.
• Patron satisfaction is important, but should not deter effective security procedures.
  – Patrons will learn to adapt, especially with effective communication provided to them.

Image credit: commons.wikimedia.org
Patron Satisfaction

Airport Security Survey*

1. Did you go through security screening today?
   Yes? No?

2. Do you think the amount of time it took you to get through security today was
   (please check):
   Reasonable
   Longer than reasonable
   Shorter than reasonable

3. How would you rate the courtesy and professionalism of the security officials you encountered at the airport screening checkpoint?
   Very courteous / professional
   Somewhat courteous / professional
   Somewhat discourteous / unprofessional
   Very discourteous / unprofessional

4. When going through security, were you selected for additional screening?
   Yes
   No

Patron Satisfaction

5. If selected for additional screening today, please mark which of these additional measures you went through: (please mark any which occurred – you may mark more than one)
   Security officer used a metal detector wand and scanned your entire person
   Security officer ran a swab / cloth over your belongings
   Security officer opened your bag and looked inside of it without removing contents
   Security officer opened your bag and removed some / all of its contents
   Security officer opened and tested a liquid or gel in your bag
   Other, please describe here:
   ____________________________________________________

6. If you were selected for further screening, did security officials explain why you were selected for further screening?
   Yes  Please write the reason they gave you here:
   ________________________________________
   No

7. If you were selected for further screening, why do you feel you were selected? ________
Patron Satisfaction

- The literature on patron satisfaction can inform the choice of randomization protocols.
- Perceived fairness is central to patron satisfaction.
- The theory of service fairness tells us: Organizations failing to project an image of service fairness cannot develop the level of customer confidence needed to establish loyalty.
- Implication: It is critical to:
  - Introduce randomization in such a way that perceived service fairness is kept in mind.
  - Train security personnel to apply a randomization process properly.
Patron Satisfaction

• It is also important to train security to show empathy and explain/demonstrate the randomized nature of a process.
• An intriguing idea is to reframe the way patrons perceive random selection from bad to good luck.
• We might do this by finding at least small ways to compensate those chosen for extra screening with a “reward” such as entry into a lottery.
Implementing Randomization

• How is randomization best implemented so as to be:
  – Efficient
  – Effective
  – Unbiased
  – Minimize the perception of unfairness/bias

Credit: commons.wikimedia.org
“Sophisticated” Randomization

- Sometimes randomization can be based on quite sophisticated methods
- Some well-known efforts at randomization in security involve the use of sophisticated tools of game theory based on adversary-defender games where the adversary takes advantage of some knowledge of the defender’s strategy.
- This idea has been pioneered by Milind Tambe at University of Southern California and his colleagues.
- It was first developed and implemented at LAX airport in Los Angeles.

Credit: commons.wikimedia.org
“Sophisticated” Randomization

• The work on game theory and security has led to a wide range of actual deployed applications:
  – Scheduling checkpoints and K-9 patrols at airports
  – Deploying air marshals on air carriers
  – Randomizing security activities to protect airport infrastructure
  – Scheduling randomized patrols within ports
  – Deploying escort boats to protect ferries
  – Scheduling multi-operation patrolling (fare evasion, counter-terrorism and crime) on subway trains
  – Preventing illegal, unreported, and unregulated fishing
  – Assigning randomized patrols to catch poachers in wildlife preserves

Image credits: commons.wikimedia.org
“Sophisticated” Randomization

- How it Works
- Case in point: patrolling the harbor:
  - Critical harbor infrastructure was selected.
  - Different actions at each infrastructure were identified. (Observe as you pass by, stop and watch, go inside, ⋯)
  - Values were set on critical infrastructure in the harbor.
  - The software then randomly selected a patrol path (including actions) that visits different infrastructure.
  - It placed higher priority on visiting higher valued infrastructure.
  - Different actions had different deterrent value.
  - Each path had a value (though low-valued paths could be chosen).
  - The sophistication of the game theory lies in the development of algorithms for choosing a given path each day.

Image credit: commons.wikimedia.org
“Sophisticated” Randomization

• For “sophisticated” randomization tools to be successfully implemented at sports and entertainment venues:
  – The implementation must be simple with the complex math in the background.
  – There needs to be close collaboration between technical developers and users in order to inform the complex math required to make it appropriate for a given venue.
• Simple tools of randomization are a likely best way to start implementing randomization into sports and entertainment venue security.
• These accomplish the goal of “unpredictability.”
• These can be general enough to fit many venues.
Implementing Randomization: Patron Screening

• The screening process can be time consuming, may annoy patrons, and may cause queue buildups that may create vulnerabilities.

• A simple design that randomly selects some patrons for extensive screening, but has other patrons go through quicker, less extensive checks, should be considered.

• However, even the practical implementation of a simple random selection process presents challenges.

• We surveyed leading venue security directors. Few had implemented randomization in screening as yet.
Implementing Randomization in Patron Screening

• Implementations should be unbiased and fair.
• The following are some simple implementations that appear to be unbiased and fair.
• Perhaps the simplest tool for implementing randomization may be to count every so many people and then choose the next one.
• Human counts, used by some venues, and choosing every $n^{th}$ person, may not be ideal, even if $n$ is varied from day to day.
• These are hard to implement, not transparent to patrons, and don’t leave an audit trail.

Credit: commons.wikimedia.org
Implementing Randomization in Patron Screening

• Using a deck of cards from which a patron chooses is transparent, but perhaps time-consuming to implement if used repeatedly unless the card is chosen while the person is waiting on line.
Implementing Randomization in Patron Screening

- Another tool for implementing randomization in patron screening could be to use a visible random device (e.g., a touch device that patrons can activate) to pick a certain fraction of the people for the practice.
- One can use a hidden random device to pick a certain fraction of patrons (e.g., a photocell or other counter on a WTMD).
- For the case of secondary screening, perhaps the most effective method may be to utilize a built-in feature of certain WTMDs to make a random selection for additional screening even if the WTMD detects no metal on a patron.

Image Credits: commons.wikimedia.org
Implementing Randomization in Patron Screening

• One could use random number generators on an iPad or tablet with patrons tapping the screen.
• Or use a foot-operated device that patrons would step on.

credit: commons.wikimedia.com

credit: Ruggie alarm, Amazon.com
Implementing Randomization in Patron Screening

• One could use a random approach to decide whether to do a specific practice (from a Playbook) on a given day.
• Or use a random approach to choose which prepared plan to use on a given day.
• A Playbook contains a number of security configurations (e.g., enhanced secondary inspections of patrons, use of K-9s in a given area of the loading dock), while a prepared plan is specific to a single aspect of security (such as how to use the K-9s).
Implementing Randomization in Patron Screening

• There is a continued need to identify practical and logistical issues to aid venues in finding ways to implement randomization in practice.
• While venue security directors have for the most part not implemented randomization in screening most felt new approaches could be important.
Implementing Randomization in Patron Screening

• Before implementing a new randomization component of patron screening, it would be good to understand the implications for the security manager:
  – Effectiveness: Increased security?
  – Efficiency: Decreased throughput?
  – Resource requirements?
  – Unintended consequences (e.g. increased vulnerability of patrons)?
• One can then test this in advance using a simulator.
Changes in the CCICADA Stadium Simulator

• We updated the Stadium Simulator with new processes and new options.
• Examples:
  – Different arrival rates at different times.
  – More screening processes (e.g., bag size check or explosives detection swab at “outer perimeter).
  – Randomization of different processes.
• This enabled us to use it to explore different randomization protocols.
Simulation Experiments for New Randomization Protocols

• Before actually trying out a new technology in practice, find ways to estimate the impact of that technology.
• We did this for various randomization protocols.
• Used the CCICADA Stadium Simulator to do experiments.

Image credit: commons.wikimedia.org
Simulation Experiments for New Randomization Protocols

- Need to compare a new security initiative to a “baseline” or control.
- Because of probabilities involved, have to run the simulation multiple times both for baseline and new protocol.
  - To get a feeling for the random variation.
- Results of the runs for the baseline can be compared to the runs for the experimental change.

credit: En.wikipedia.org
Simulation Experiments for New Randomization Protocols

• Need to decide what information will be most helpful.
  – The result of each run?
  – The average value of the outcomes (e.g., average time spent in security) on each baseline run vs. on each experimental run?
  – The “worst case” (longest time spent in security) on each baseline run vs. on each experimental run?
Simulation Experiments for New Randomization Protocols

• Sample experiment: *Explore the protocol of increasing the security level on one WTMD.*
• This detector will pick up more contraband.
• Arriving patrons assigned randomly to an inspection lane.
• Four inspection checks:
  – Arriving patrons screened for compliance with size of bag they brought in.
  – Bag contents check.
  – WTMD follows that.
  – Secondary inspection by wanding if WTMD sends alarm.
Simulation Experiments for New Randomization Protocols

- Some basic assumptions required for baseline and experimental protocol:
  - Patron arrival rate.
  - Number of inspection lanes.
  - For inspection step:
    - Distribution of screening times.
    - Percent of patrons with contraband.
    - Contraband detection rate.
    - False positive rate.

Image credits: commons.wikimedia.com
Simulation Experiments for New Randomization Protocols

• We assumed there were 10 security lanes.
• One with higher security setting on its WTMD.
• Assumed it detected 95% of contraband, vs. 80% for the other WTMDs.
• Assumed 1% of patrons had contraband.
• Exact assumptions not important.
• 20 simulation runs for both baseline and new protocol.
• For each simulation run, calculated average time spent in security over all patrons.
• Average of this average:
  – Baseline 2.55 minutes.
  – New protocol 3.22 minutes.
Simulation Experiments for New Randomization Protocols

- Security director would have to decide if such an increase would be acceptable in terms of potential effect on patron satisfaction.
- Increase of about 30 seconds might not seem too bad.
- But maybe need detail: what is distribution for person entering in last 20 minutes?
- Calculated overall detection rate for each run.
- Average overall detection rate:
  - Baseline 86.3%.
  - New protocol 87.1%.
- Seems like a minor gain in exchange for a relatively minor loss in average inspection time.
Simulation Experiments for New Randomization Protocols

• Next, for each run, calculated how many people were in security lines when that number was as large as possible.

• It is a measure of vulnerability caused by security.

• Average of the maximum number in security:
  – Baseline: 941.
  – New protocol: 1,087.

• In sum: minor increase in detection rate vs. relatively minor increase in average time in inspection and moderate increase in vulnerability.

• Note: average wait time in higher security setting lane was 9.34 minutes, but detection rate was 94.3%.

credit: commons.wikimedia.com
Simulation Experiments for New Randomization Protocols

• Don’t reject an idea on the basis of one experiment.
• Not enough to conclude that the strategy of setting the security level on one or more WTMDs higher is a bad idea.
• The conclusion depends heavily on the parameters used.
• This example simply illustrates the point that such experimentation before rolling out a new security initiative is a good idea.
Simulation Experiments for New Randomization Protocols

• We looked at queue clearance time, the time after event start ("kickoff time") that the last person in line got into the event.

• Average queue clearance time over all runs:
  – Baseline: 6.60 minutes after event start.
  – New protocol: 15.70 minutes after event start.

• Why such a big increase?
• Because our model wouldn’t allow someone to switch out of a security lane - even if the line was moving much more slowly than others.
• If we didn’t allow switching, there would be some very unhappy patrons.
• Suggests rethink the simulator.
Randomization in Employee Background Checks: Briefly Visited

• Almost all large sports and entertainment venues do an initial background check on employees.
• Arrests, restraining orders from courts, etc. are not typically available to employers.
• This suggests doing rechecks.
• Few do rechecks because of the expense.
• Doing rechecks randomly can lower the cost and also act as a deterrent.

credit: commons.wikimedia.com
Randomization in Employee Background Checks: Briefly Visited

• In contrast to the situation with randomization protocols for security inspection, there is a lot of experience with randomization in employee screening.
• Much of this involves rechecking for drug use or similar problems.
• “Best practices” for fair and unbiased rechecks have been developed over the years.
• Actual implementation should reflect the principles discussed under avoiding perception of bias:
  – Provide information about rechecks, be transparent, etc.

Image credit: National Institute of Drug Abuse
Selected Best Practices in Randomization in Employee Background Checks

• Conduct randomized rechecks over a defined time period, ensuring that each employee is selected at least once by the end of the period.

• Some subtlety:
  – Suppose 300 employees and every employee has 1/3 chance to be picked even if they were picked last year.
  – Suppose we *randomly* do a background screening on 1/3 of the employees every year.
  – Year 1 misses 200 of them, Year 2 misses about 2/3 of that 200 or about 133, and Year 3 still misses about 2/3 of that 133 or about 86.
  – So, in 3 years, ~86 are *never* checked.
  – Perhaps one needs some sort of hybrid plan that requires checking those who are omitted by the randomization.
Selected Best Practices in Randomization in Employee Background Checks

• Randomly select employees for more in-depth background screening.
• Random selection methods should be scientifically valid and the randomness of the selection method must be verifiable.
• Ensure employee privacy.
• Do not discard a selection without adequate explanation.
• Distribute the tests reasonably throughout the year.
• Refresh the pool of employees before each random selection.
• Retain and maintain records and maintain testing pool.
Thanks to the other Members of the CCICADA Research Team

• Michael Alles, Rutgers University
• Jonathan Bullinger (research associate)
• Terri Adams-Fuller, Howard University
• Dennis Egan, Rutgers University
• Paul Kantor, Rutgers University
• Christie Nelson, Rutgers University
• Shannell Thomas, Howard University (student)
• Sevincgul Ulu, Rutgers University (student)
• Can Uslay, Rutgers University
• Ryan Whytlaw (research associate)
• Cheng Yin, Rutgers University (student)
• Michael Young (consultant)