The Economics of Hardware Security

Thesis Proposal | 2023 December 11

Adam Hastings


Could Disrupt American Military Operations
American intelligen
China the power to
resupply operation
Home News Research Board Pack Newsletters Events
SHARE
WSJ PRO
Critical Infrastructure Companies Warned to Watch for Ongoi
Cyberattack
Hackers exploited a 'zero-day' flaw in Ivanti software to breach 12 ministries in Norway
REUTERS
World Business Markets Sustainability Legal Breakingviews Technology Investigations
World More
U.S. Justice Department says its emails were breached by SolarWinds hackers
10 PM EST · Updated 3 years ago
MUST READS FR
1. EU Advances Data-Flow De After U.S. Mak Surveillance Changes
2. European Elect
Security
Okta admits hackers accessed data on all customers during recent breach
The New York Times
Capital One Data Breach Compromises Data of Over 100 Million
Share full article
475
The New York Times
Cyberattack Forces a Shutdown of a Top U.S. Pipeline
The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.
abc NEWS VIDEO LIVE SHOWS ELECTION 2024 538
Ransomware attack prompts multistate hospi
chain to divert some emergency room

2023 CWE Top 25 Most Dangerous Software Weaknesses (MITRE)

1. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1
2. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3
4. Use After Free
   CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲
5. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
   CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲
6. Improper Input Validation
   CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼
7. Out-of-bounds Read
   CWE-125 | CVEs in KEV: 2 | Rank Last Year: 5 (down 2) ▼
8. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
   CWE-22 | CVEs in KEV: 16 | Rank Last Year: 8
9. Cross-Site Request Forgery (CSRF)
   CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9
10. Unrestricted Upload of File with Dangerous Type
    CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

2023 CWE Top 25 Most Dangerous Software Weaknesses (MITRE)

1. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1
   Aka buffer overflow
2. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3
4. Use After Free
   CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲
5. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
   CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲
6. Improper Input Validation
   CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼
7. Out-of-bounds Read
   CWE-125 | CVEs in KEV: 2 | Rank Last Year: 5 (down 2) ▼
8. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
   CWE-22 | CVEs in KEV: 16 | Rank Last Year: 8
9. Cross-Site Request Forgery (CSRF)
   CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9
10. Unrestricted Upload of File with Dangerous Type
    CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

2023 CWE Top 25 Most Dangerous S…RE)

1	Out-of-bounds Write	CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1
2	Improper Neutralization of Input During Web P…	CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2
3	Improper Neutralization of Special Elements us…	CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3
4	Use After Free	CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲
5	Improper Neutralization of Special Elements us…	CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲
6	Improper Input Validation	CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼
7	Out-of-bounds Read	CWE-125 | CVEs in KEV: 2 | Rank Last Year: 5 (down 2) ▼
8	Improper Limitation of a Pathname to a Restri…	CWE-22 | CVEs in KEV: 16 | Rank Last Year: 8
9	Cross-Site Request Forgery (CSRF)	CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9
10	Unrestricted Upload of File with Dangerous Typ…	CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10

Aka buffer ove…

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

Buffer overflows: attacks and defenses for the vulnerability of the decade

Publisher: IEEE | Cite This | PDF

C. Cowan ; F. Wagle ; Calton Pu ; S. Beattie ; J. Walpole **All Authors**

82	5	2339
Cites in Papers	Cites in Patents	Full Text Views

Abstract | Authors | References | Citations | Keywords | Metrics

Abstract:
Buffer overflows have been the most common form of security vulnerability for the last ten years. Moreover, buffer overflow vulnerabilities dominate the area of remote network penetration vulnerabilities, where an anonymous Internet user seeks to gain partial or total control of a host. If buffer overflow vulnerabilities could be effectively eliminated, a very large portion of the most serious security threats would also be eliminated. We survey the various types of buffer overflow vulnerabilities and attacks and survey the various defensive measures that mitigate buffer overflow vulnerabilities, including our own StackGuard method. We then consider which combinations of techniques can eliminate the problem of buffer overflow vulnerabilities, while preserving the functionality and performance of existing systems.

Published in: Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00

Date of Conference: 25-27 January 2000

INSPEC Accession Number: 6498853

2023 CWE Top 25 Most Dangerous S…RE)

1 Out-of-bounds Write
CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1

Aka buffer ove…

2 Improper Neutralization of Input During Web P…
CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2

3 Improper Neutralization of Special Elements us…
CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3

4 Use After Free
CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲

5 Improper Neutralization of Special Elements us…

9 Cross-Site Request Forgery (CSRF)
CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9

10 Unrestricted Upload of File with Dangerous Typ…
CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

Buffer overflows: attacks and defenses for the vulnerability of the decade

Publisher: IEEE | Cite This | PDF

C. Cowan ; F. Wagle ; Calton Pu ; S. Beattie ; J. Walpole All Authors

82 Cites in Papers | 5 Cites in Patents | 2339 Full Text Views

Abstract | Authors | References | Citations

Abstract:
Buffer overflows have been the most common form of security vulnerability for the last ten years. Moreover, buffer overflow vulnerabilities dominate the area of remote network penetration vulnerabilities, where an anonymous Internet user seeks to gain partial or total control of a host. If buffer overflow vulnerabilities could be …ated, a very large portion of the most serious security …s be eliminated. We survey the various types of buffer …bilities and attacks and survey the various defensive …itigate buffer overflow vulnerabilities, including our own …hod. We then consider which combinations of …eliminate the problem of buffer overflow vulnerabilities, … the functionality and performance of existing systems.

…roceedings DARPA Information Survivability Conference and Exposition. DISCEX'00

Date of Conference: 25-27 January 2000

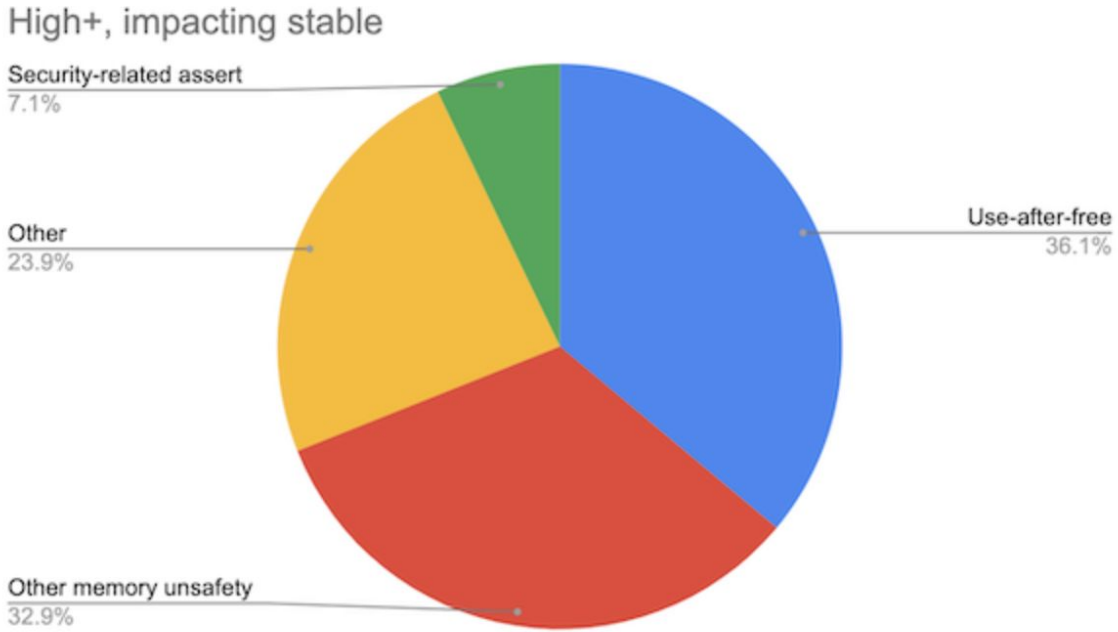
INSPEC Accession Number: 6498853

Date of Conference: 25-27

January 2000

Most real-world bugs are avoidable

"Around 70% of our high severity security bugs are memory unsafety problems (that is, mistakes with C/C++ pointers). Half of those are use-after-free bugs."



https://www.chromium.org/Home/chromium-security/memory-safety/

If we have the ability to defend against attacks, why don't we?

- Security comes at a cost (especially hardware security)
- The cost can be "paid" in many different ways by different people
- Those who can pay the cost might not have an incentive to do so
- We don't know which security tradeoffs are worth making

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

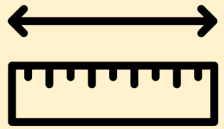
Establish a **foundation** for discussing and understanding hardware security tradeoffs

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

Conduct experiments to **measure** important security tradeoffs



Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020)*
Adam Hastings, Simha Sethumadhavan

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

Design a **mechanism** to actuate desired security tradeoffs

Talk Outline

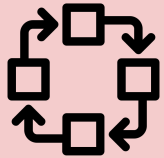
A New Doctrine for Hardware Security (*ASHES 2020)*
Adam Hastings, Simha Sethumadhavan

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

Build **models** to better understand security tradeoffs

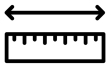


Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020)*
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

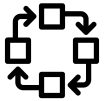


measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan



modeling

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

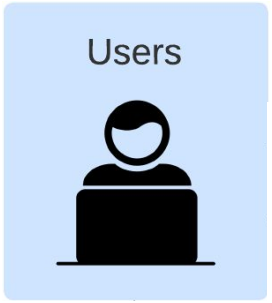
Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '24, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

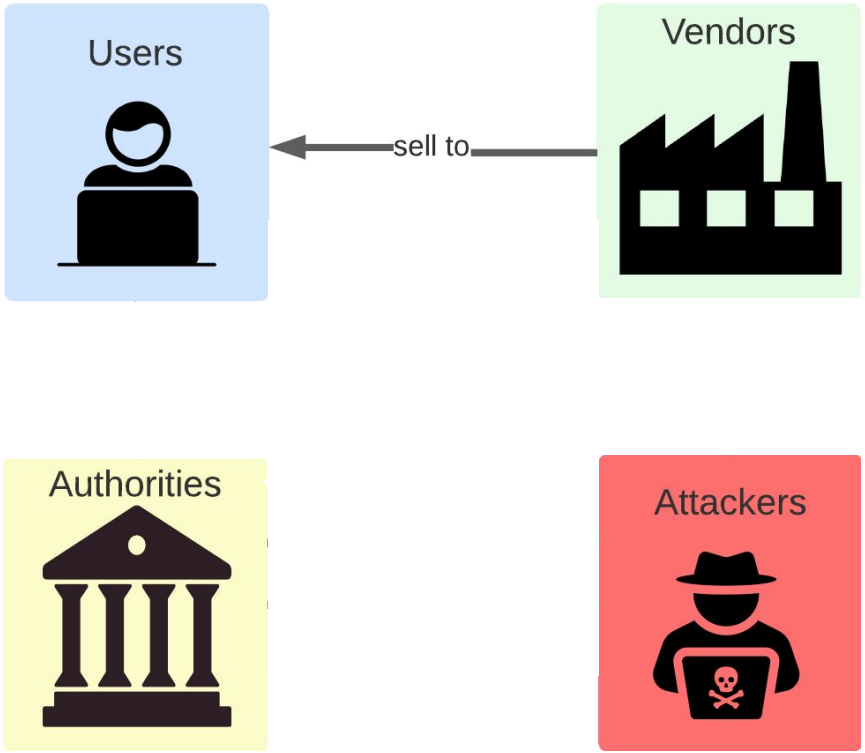
Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

modeling

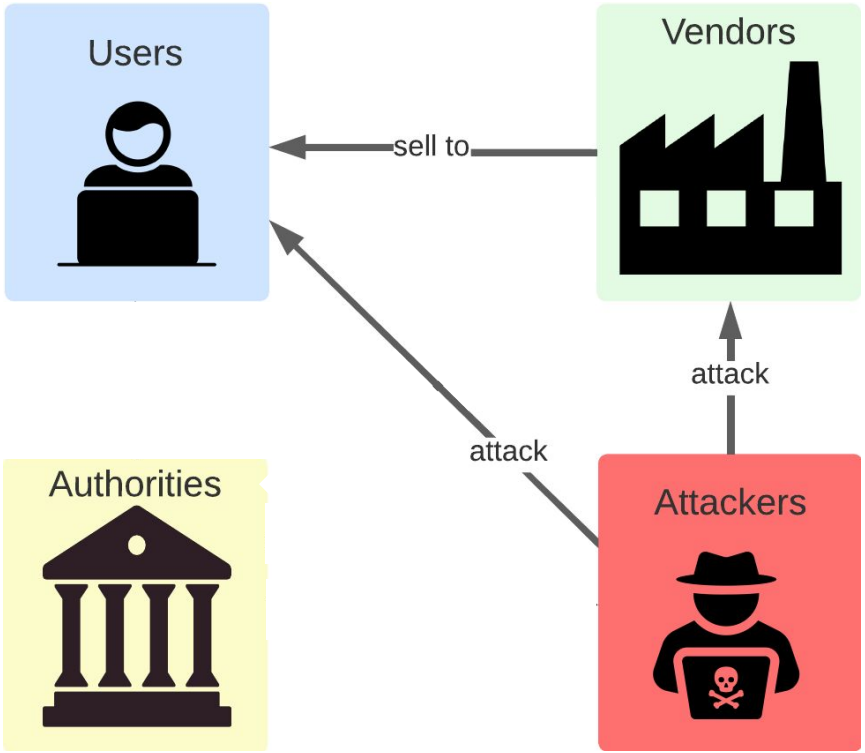
Identifying stakeholders in security



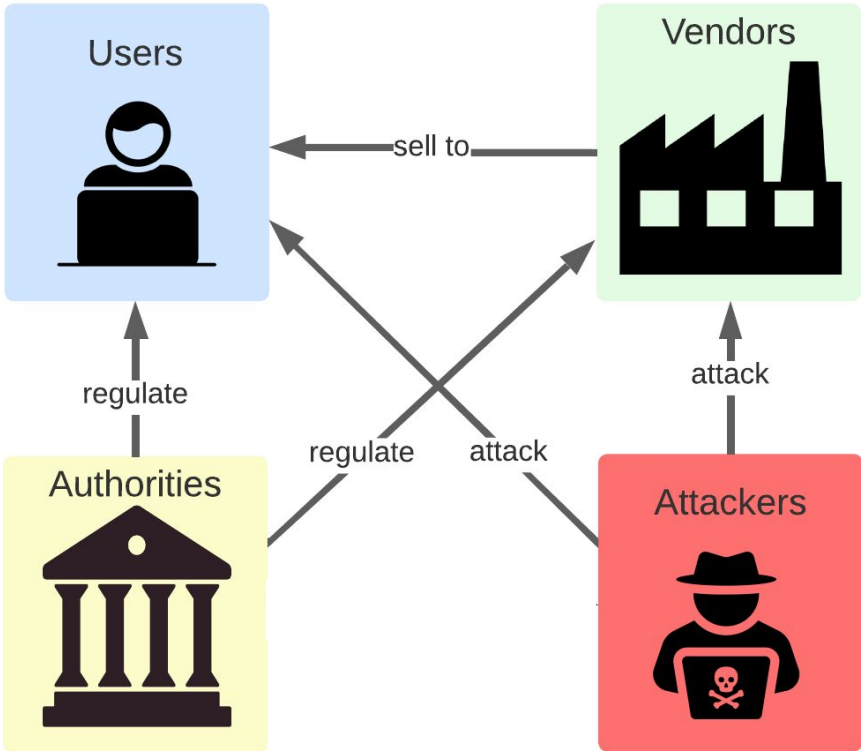
Identifying stakeholders in security



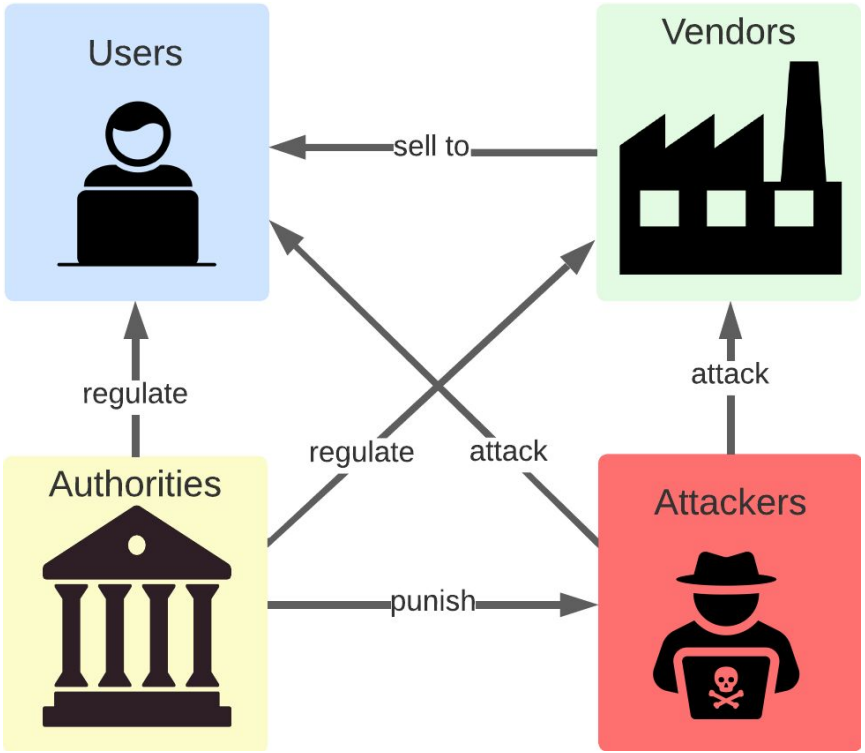
Identifying stakeholders in security



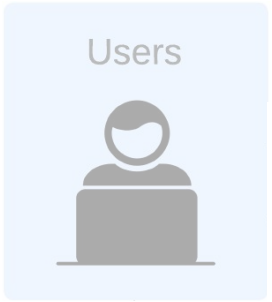
Identifying stakeholders in security

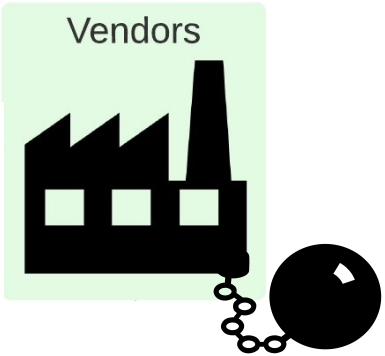


Identifying stakeholders in security

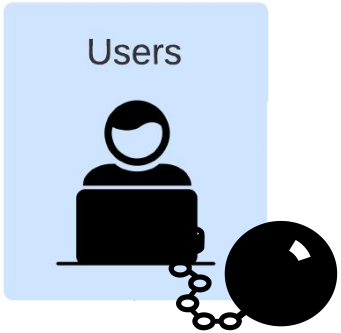


“Not my problem” → moral hazard

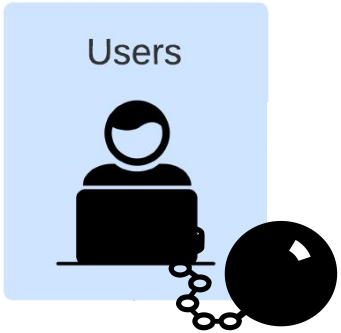




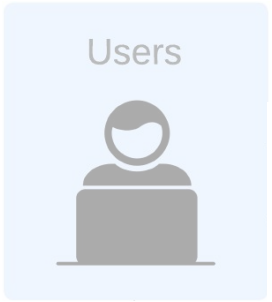
“Not my problem” → moral hazard



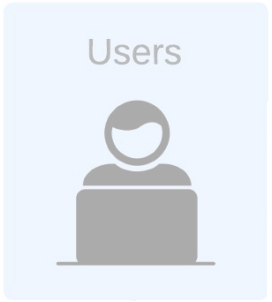
Information asymmetry → inefficient markets



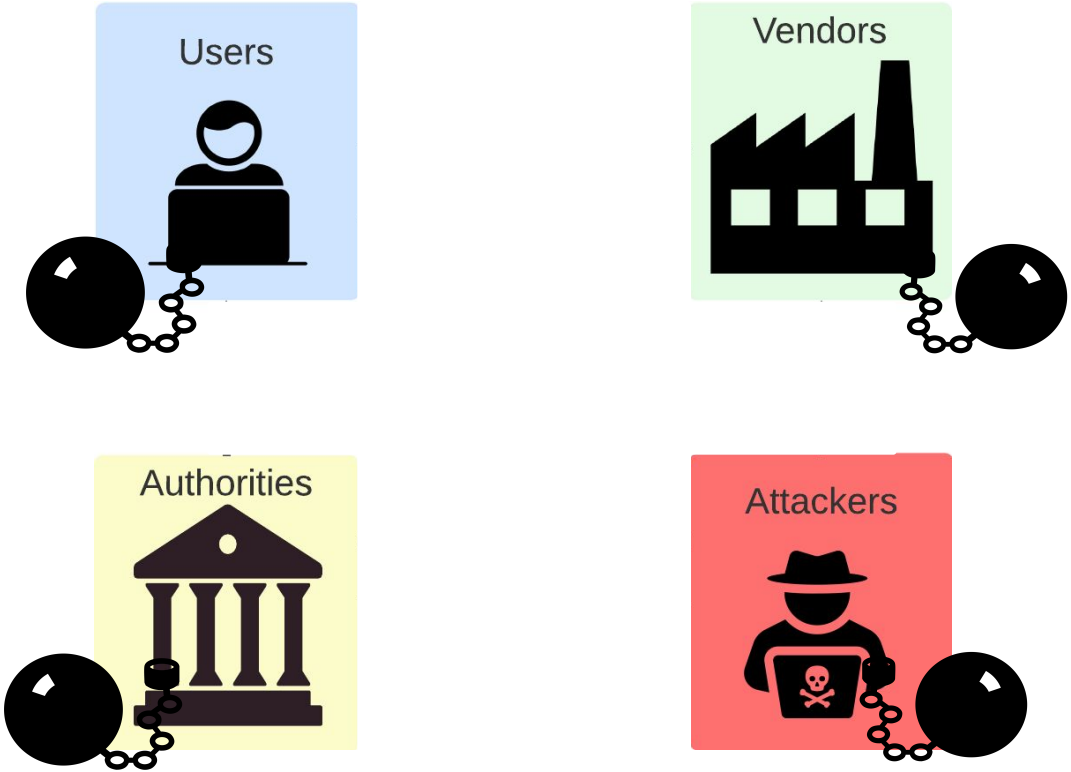
Centrally-administered security is also inefficient



Security via deterrence is preferred (but unachievable)

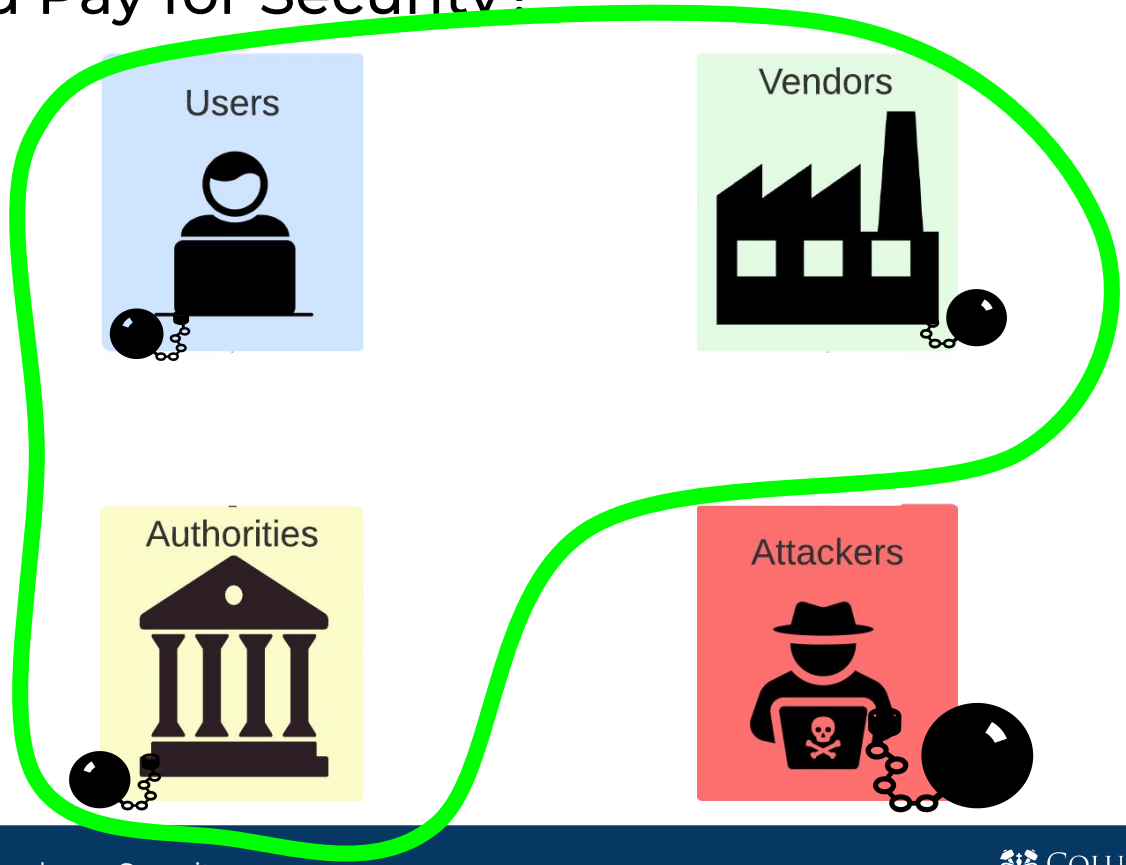


Who Should Pay for Security?

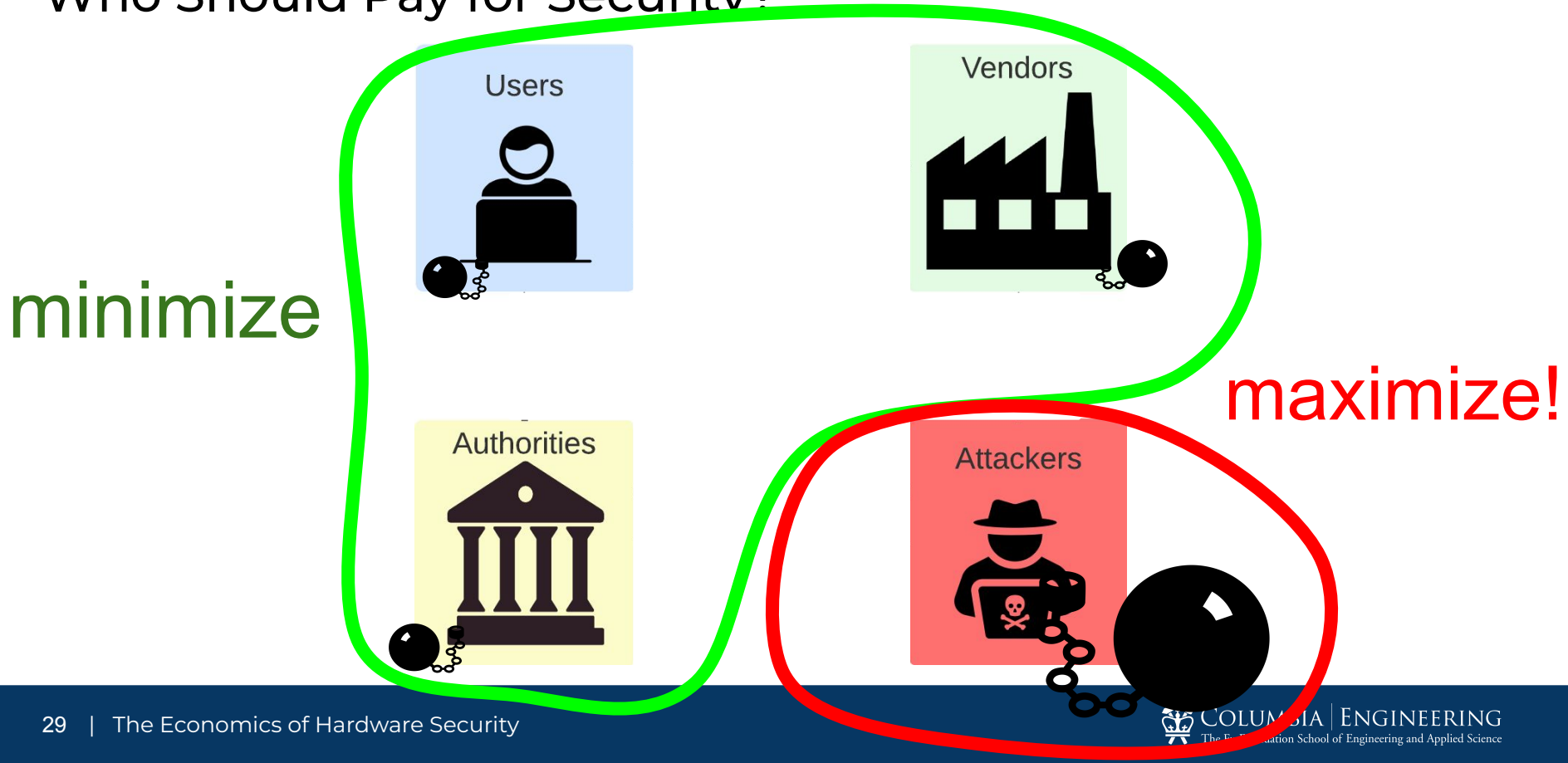


Who Should Pay for Security?

minimize



Who Should Pay for Security?



Who Should Pay for Security?

A Doctrine for Hardware Security

The burden of security should be **shared** between Users, Vendors, and Authorities.
The burden should be asymmetrically placed onto Attackers when possible.

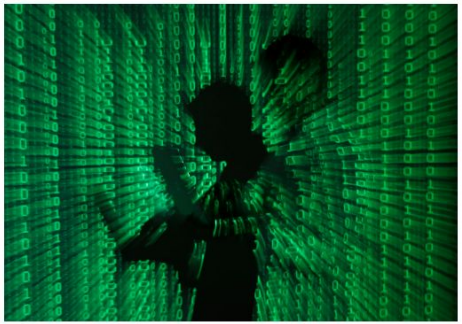
FOREIGN AFFAIRS

Current Issue Archive Books & Reviews Podcast Newsletters

Stop Passing the Buck on Cybersecurity

Why Companies Must Build Safety Into Tech Products

By Jen Easterly and Eric Goldstein February 1, 2023

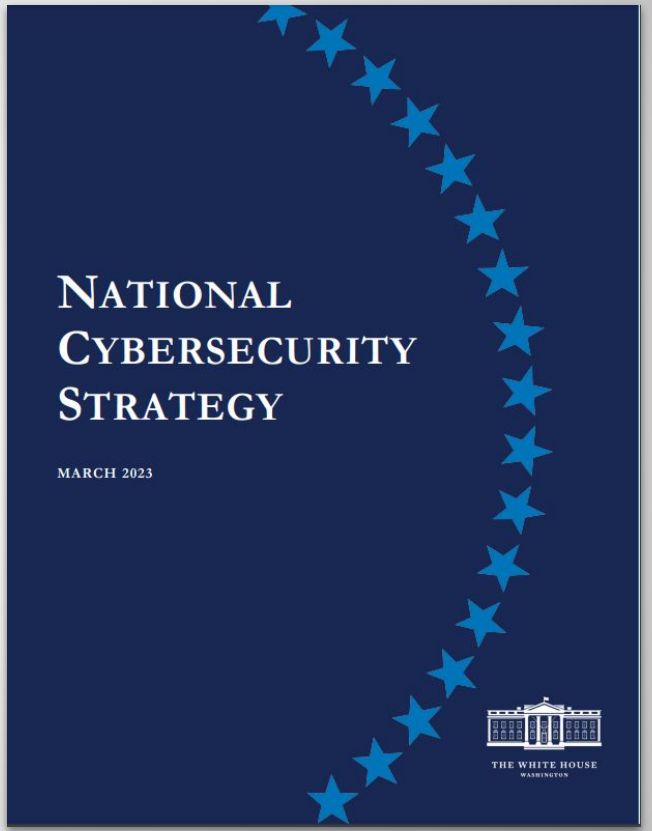


A man holding a laptop computer in Warsaw, June 2013

Kacper Pempel / Reuters

Play

Despite a global multibillion-dollar cybersecurity industry, the threat from malicious cyber-activity, from both criminal and state actors, continues to grow. While many cyber incidents

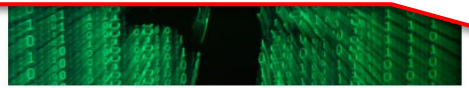


FOREIGN AFFAIRS

President Biden has made clear that all Americans deserve the full benefits and potential of our digital future. The Biden-Harris Administration's recently released National Cybersecurity Strategy ↗ calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace:

1. Ensuring that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk

2. Increasing incentives to favor long-term investments into cybersecurity

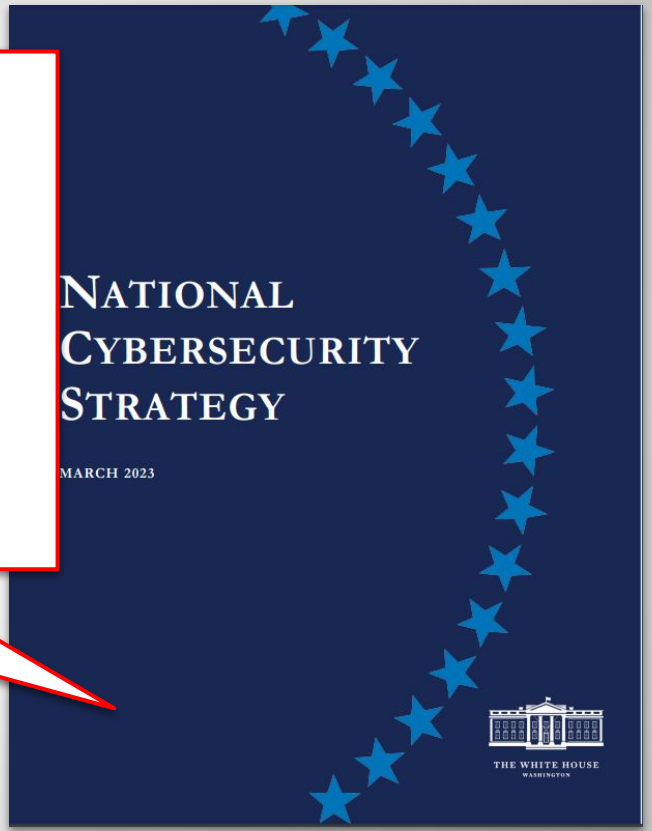


A man holding a laptop computer in Warsaw, June 2013

Kacper Pempel / Reuters

Play

Despite a global multibillion-dollar cybersecurity industry, the threat from malicious cyber-activity, from both criminal and state actors, continues to grow. While many cyber incidents



Applying Doctrine of Shared Burdens in Practice

- Case studies can help show what problems need solving
  - Memory safety, speculation safety, Rowhammer, etc.

Applying Doctrine of Shared Burdens in Practice

- Many unanswered questions….
  - How can costs/burdens be applied fairly?
  - What are the effects of our policy decisions?
  - Which tradeoffs are worth making?
  - What does enforcing a burden look like?

Applying Doctrine of Shared Burdens in Practice

- Many unanswered questions….
  - How can costs/burdens be applied fairly?
  - What are the effects of our policy decisions?
  - Which tradeoffs are worth making?
  - What does enforcing a burden look like?

These are questions that computer architects must solve. But these questions cannot be answered using techniques from computer architecture!

Thesis Statement

To make meaningful improvements to hardware security, computer architects must engage in the interdisciplinary elements of security like usability, economics, and policy.

My work is the first attempt to unify these fields by framing security as a cost.

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyberinsurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

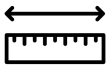
modeling

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan



measurements

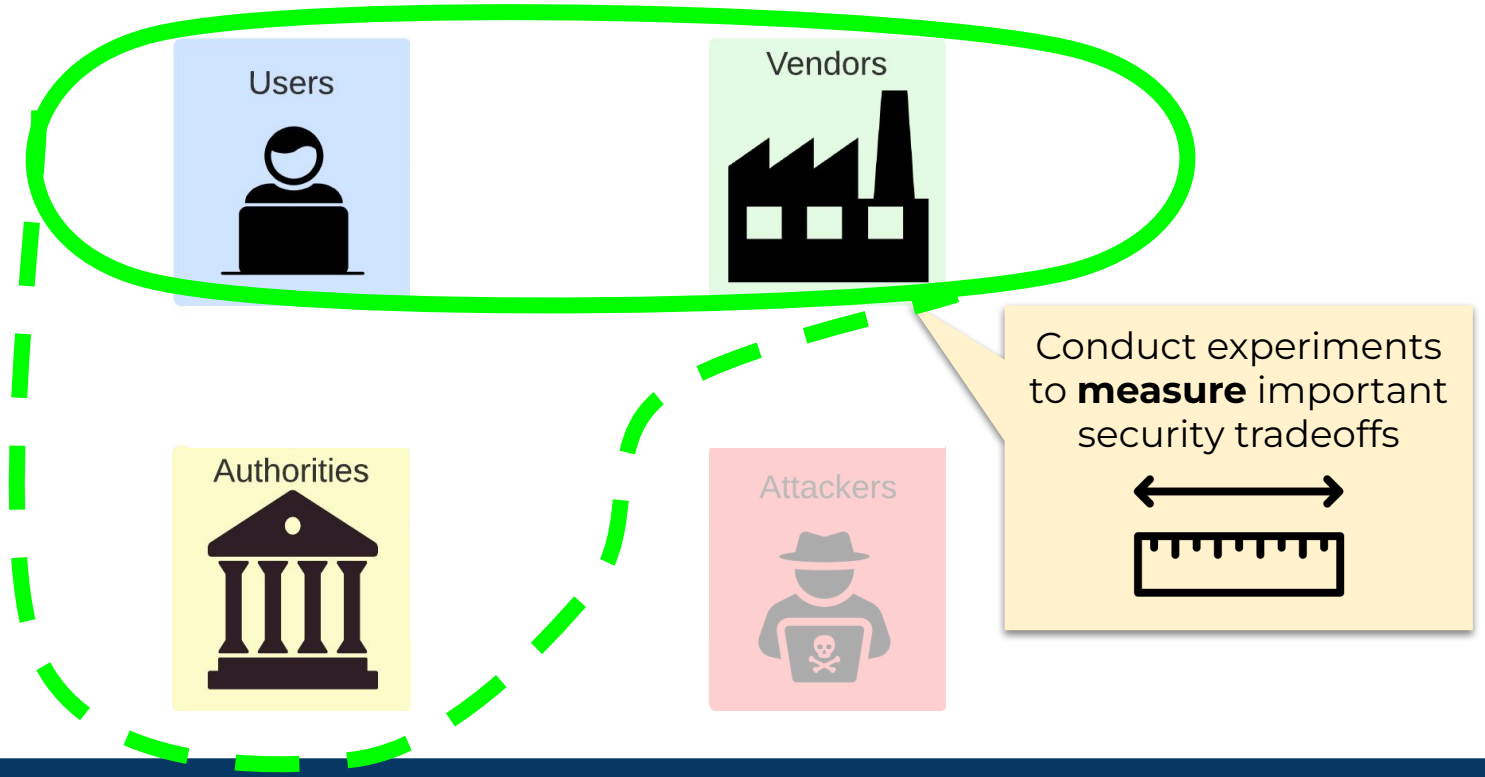
Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

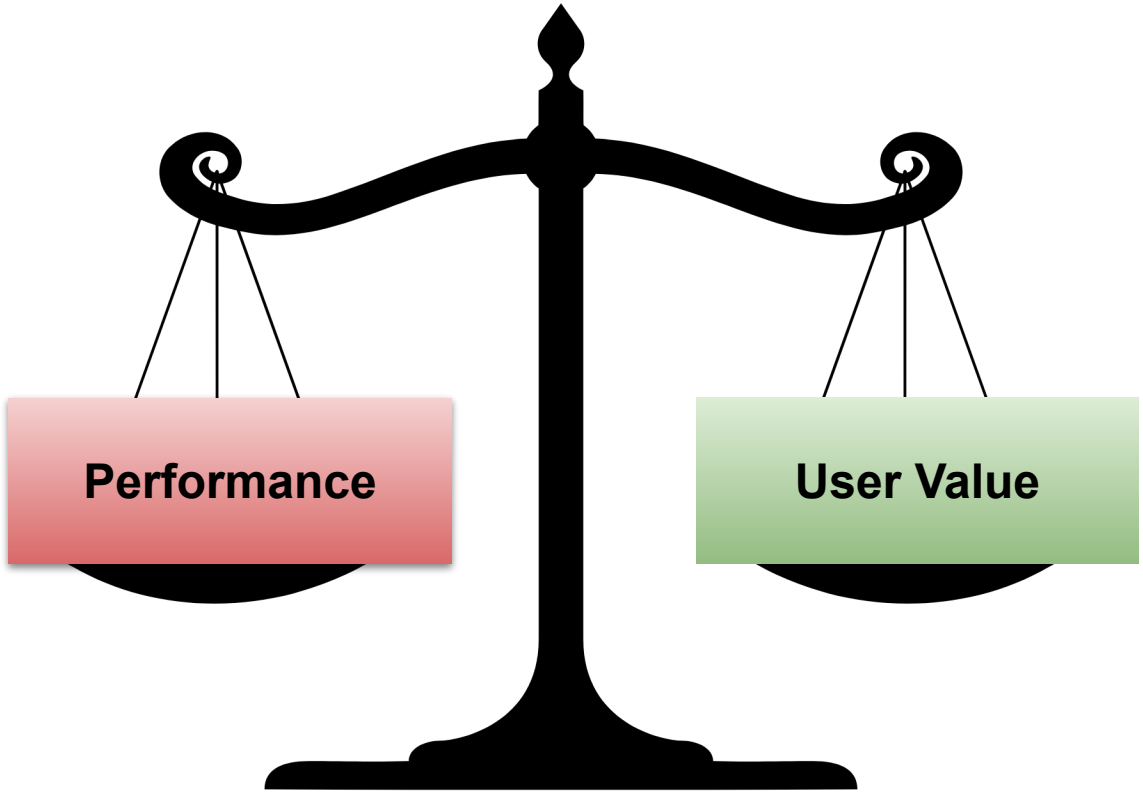
Simulations of Cyberinsurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

modeling

How Much is Performance Worth to Users?



Goal: Find “Exchange Rate” between Performance and User Value



What does the value of performance have to do with security?

1. If a vendor exchanges performance for security, how “bad” is this to users?

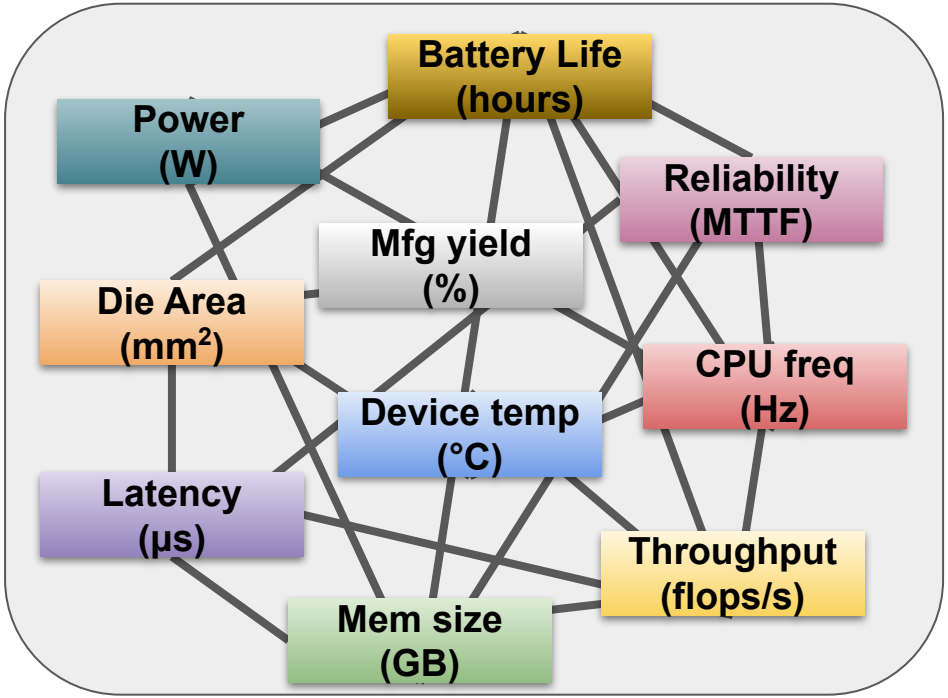
   Recall: Information asymmetry → users won’t see value in added security

   (but see negative value in lost performance!)

2. How much do hardware patches harm users?

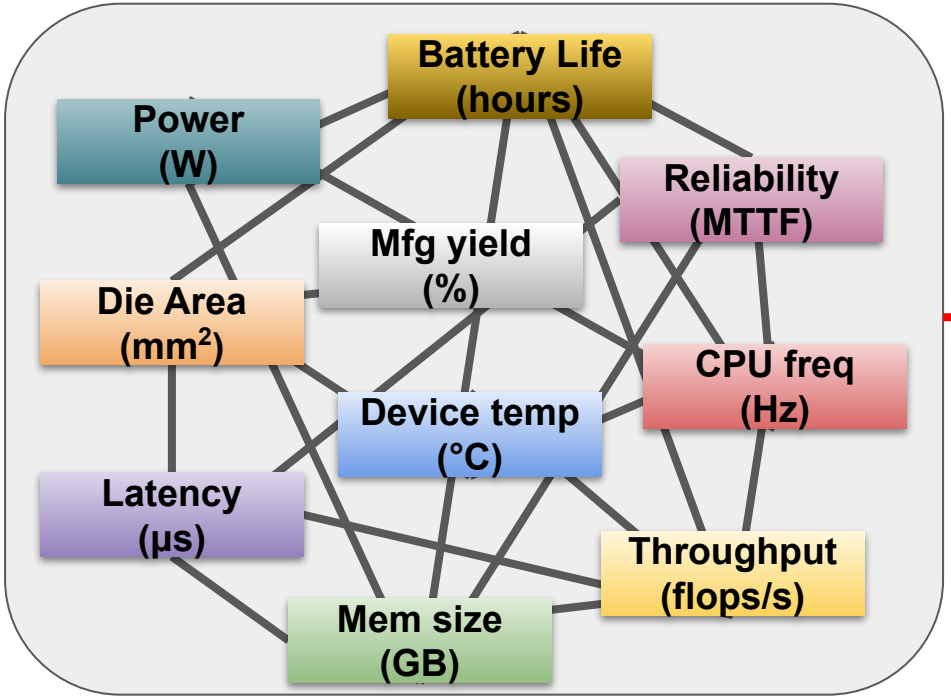
   Many patches are not deployed because of the performance hit

Bridging Quantitative and Qualitative Constraints

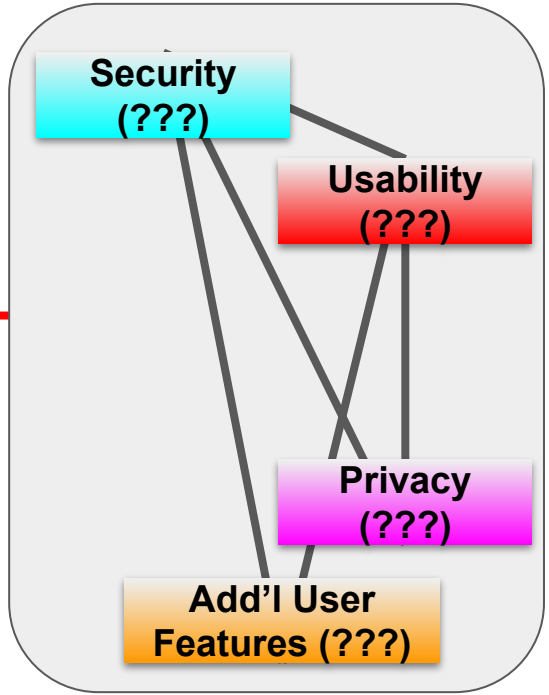


Quantitative Constraints

Bridging Quantitative and Qualitative Constraints



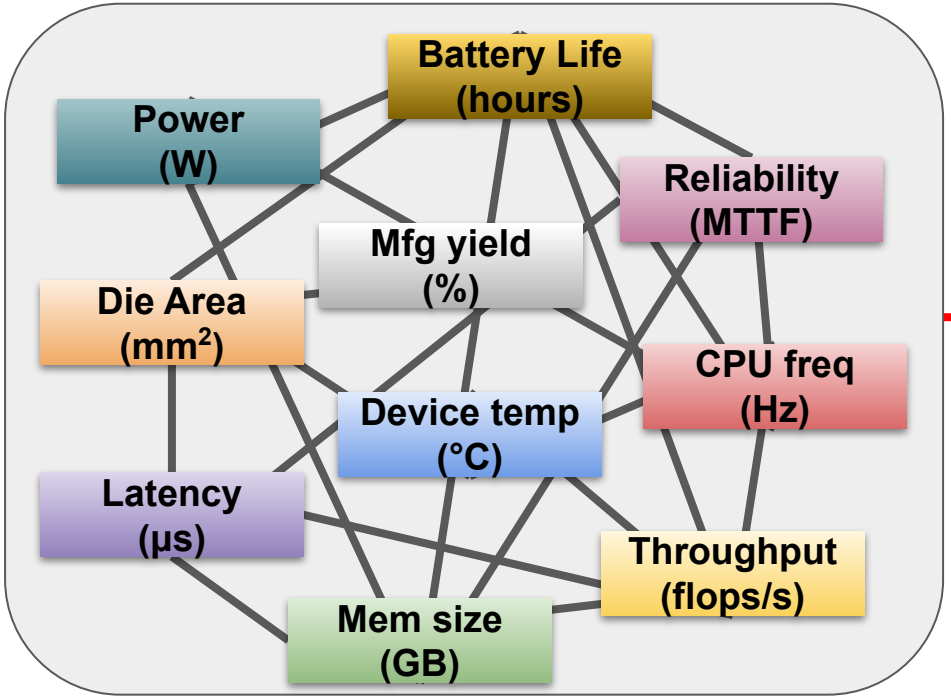
???



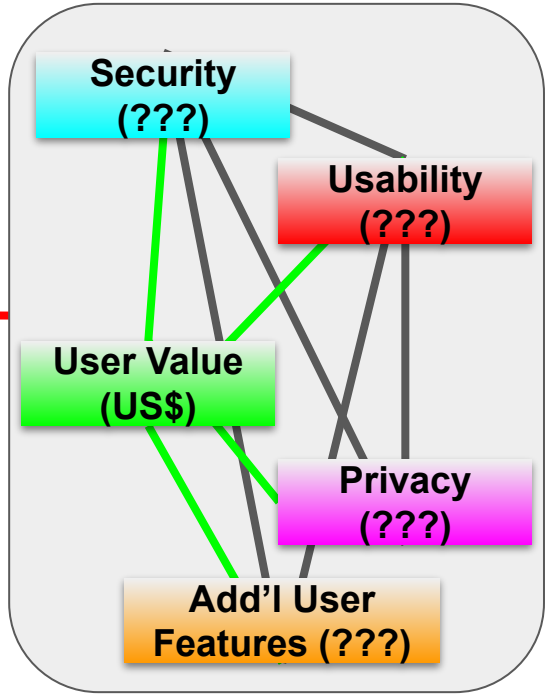
Quantitative Constraints

Qualitative Constraints

Bridging Quantitative and Qualitative Constraints



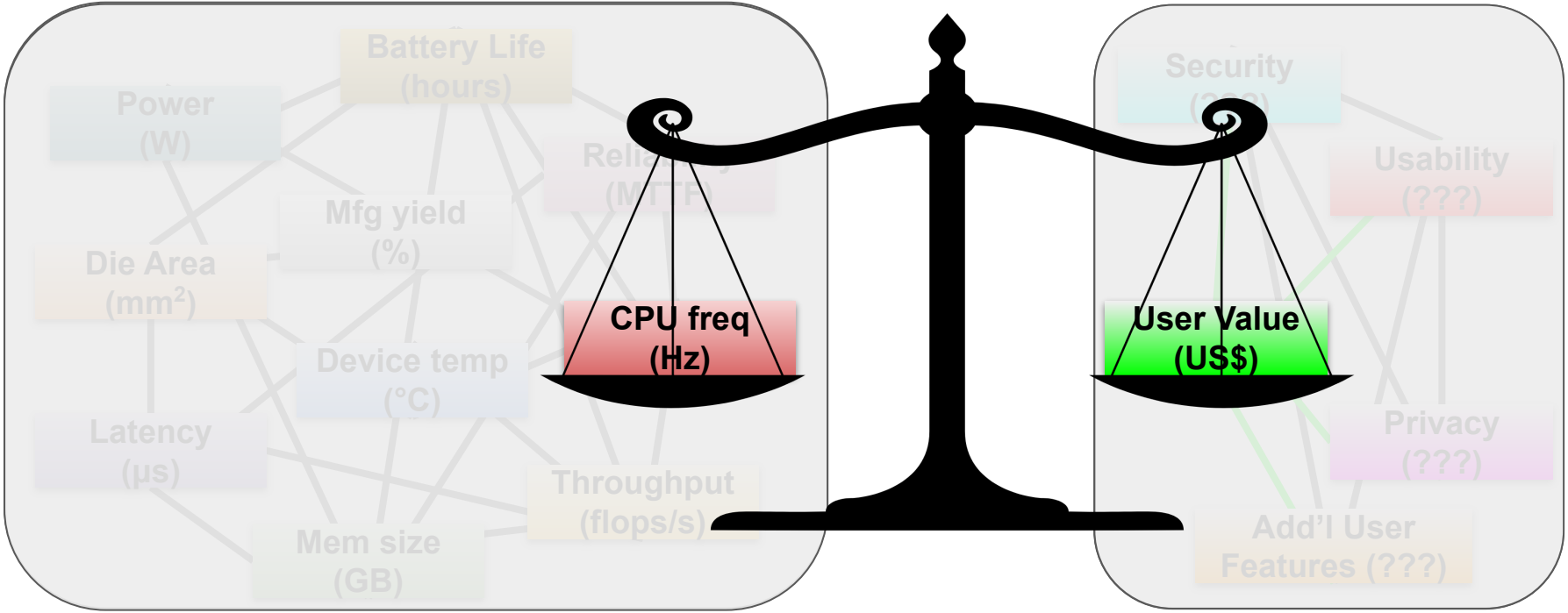
???



Quantitative Constraints

Qualitative Constraints

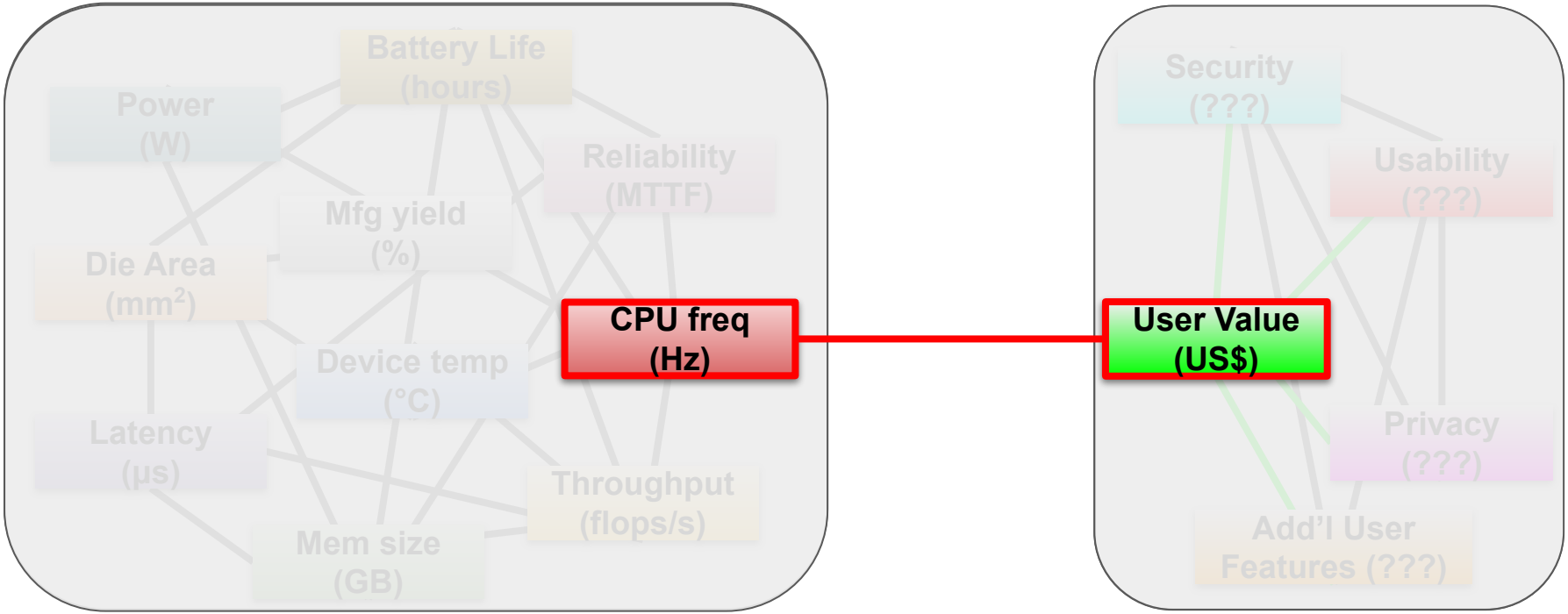
Bridging Quantitative and Qualitative Constraints



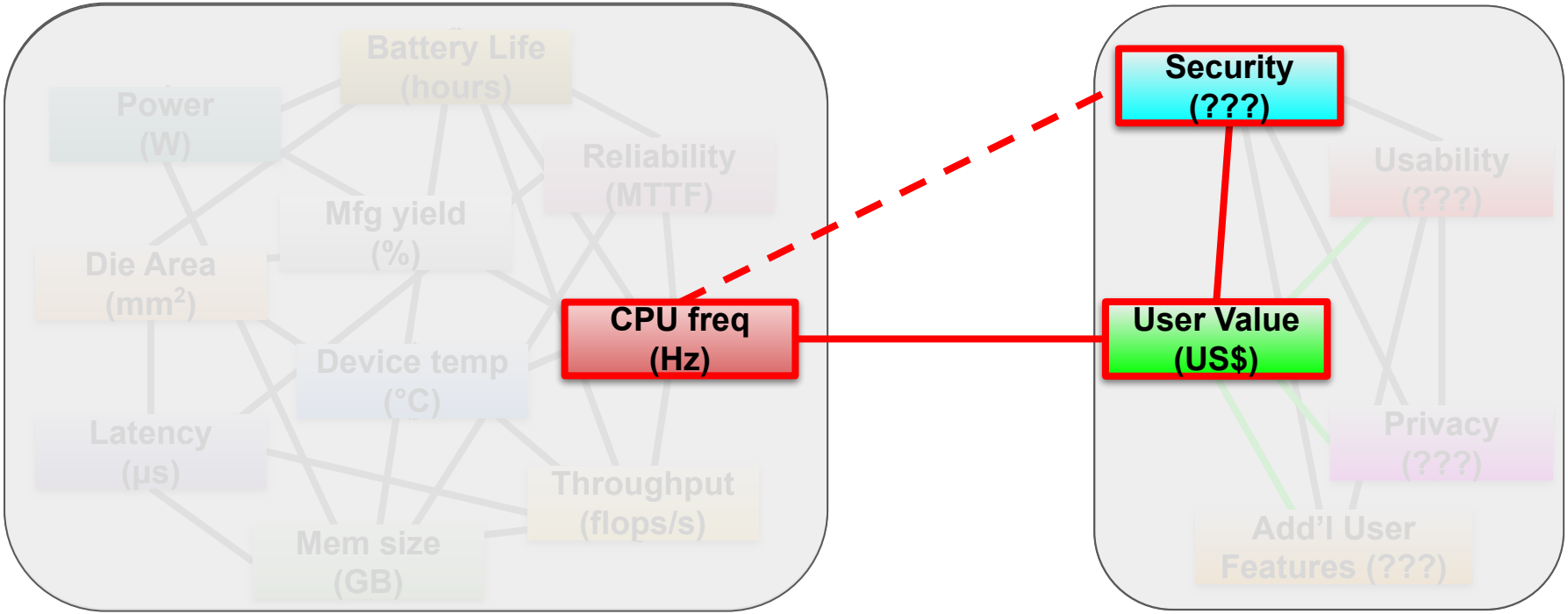
Quantitative Constraints

Qualitative Constraints

Bridging Quantitative and Qualitative Constraints



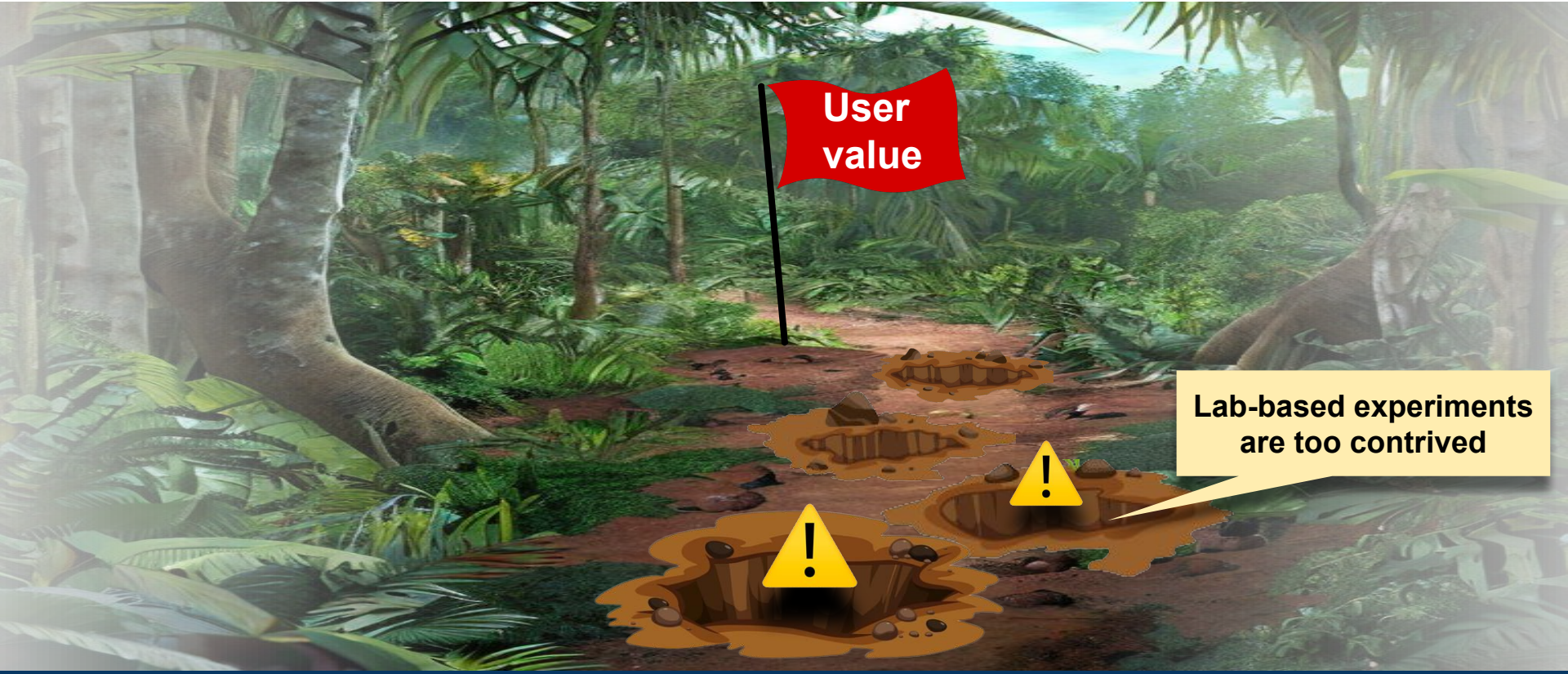
Bridging Quantitative and Qualitative Constraints



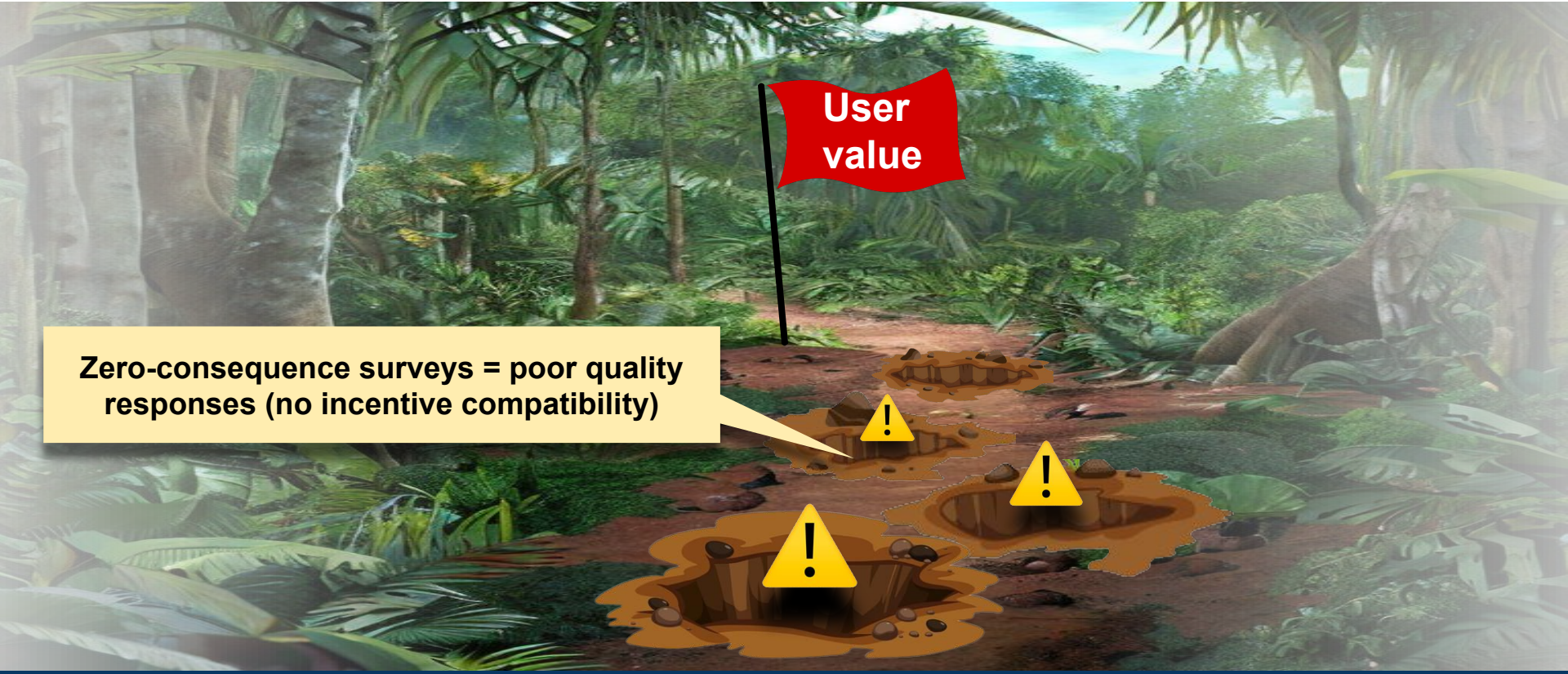
Quantifying user value is full of pitfalls

Quantifying user value is full of pitfalls

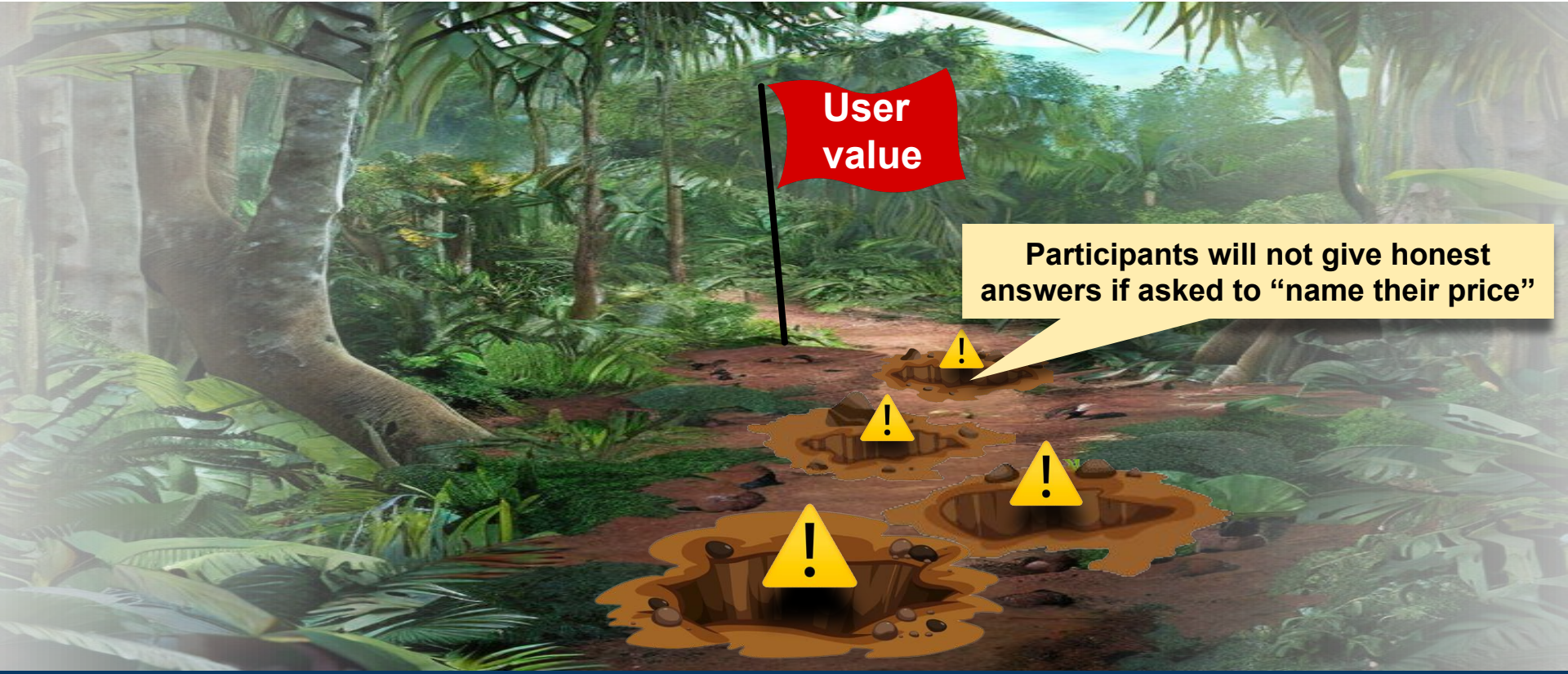
Quantifying user value is full of pitfalls



Quantifying user value is full of pitfalls



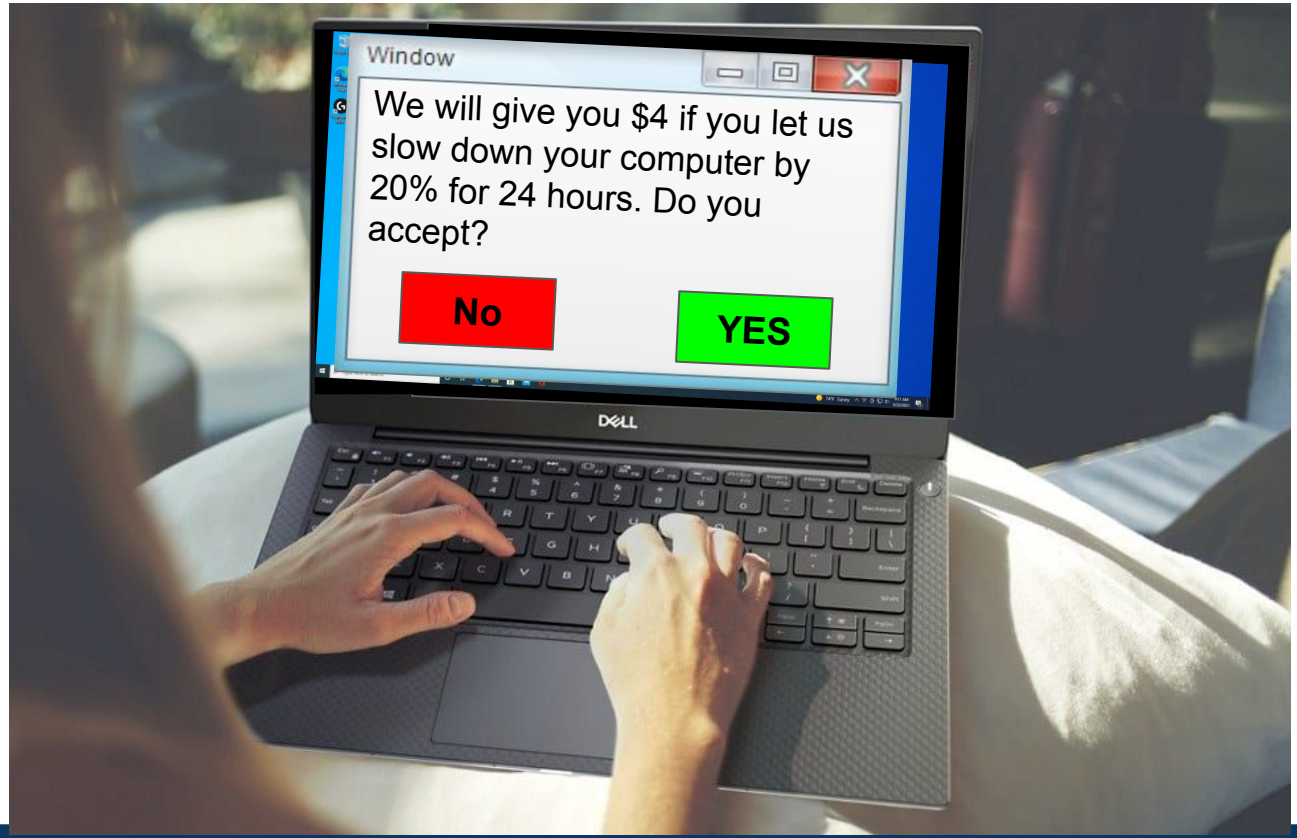
Quantifying user value is full of pitfalls



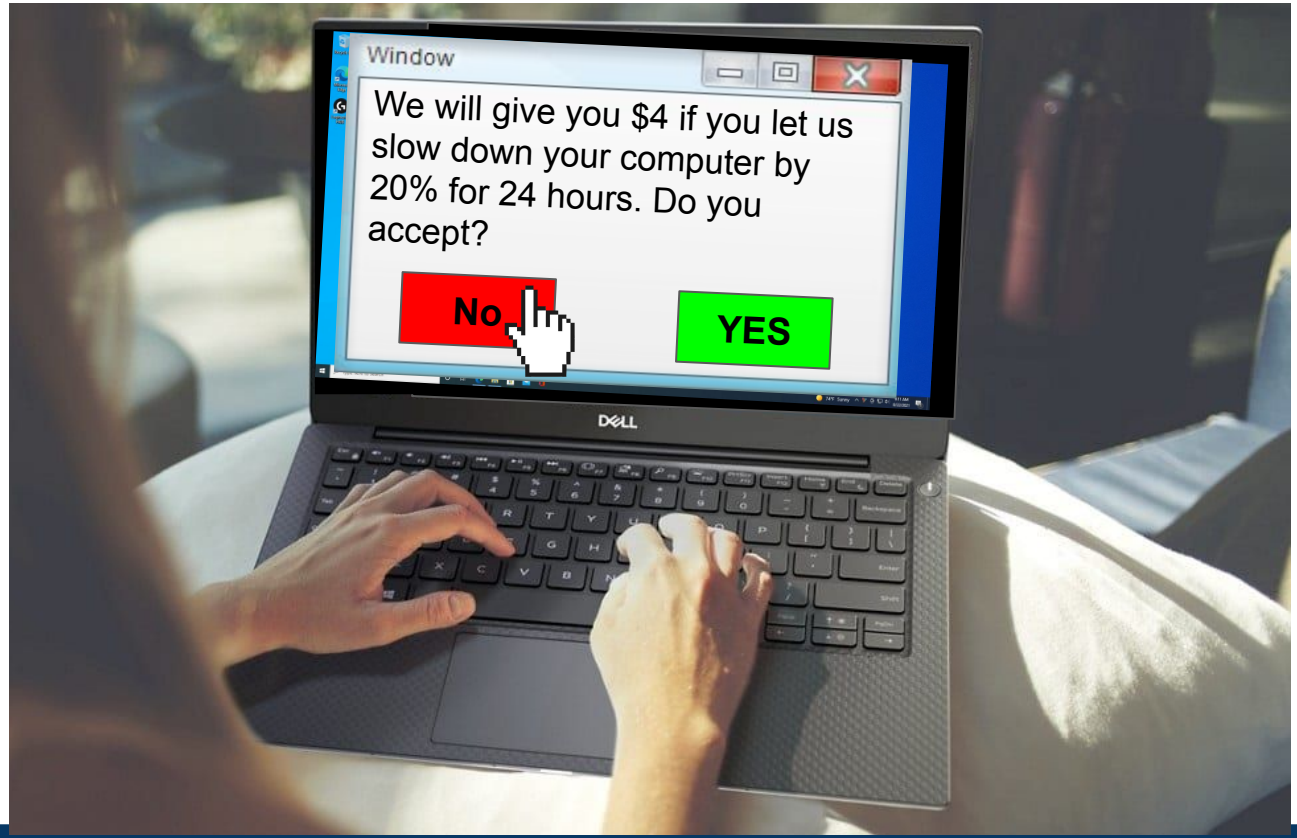
Experimental Protocol

Experimental Protocol

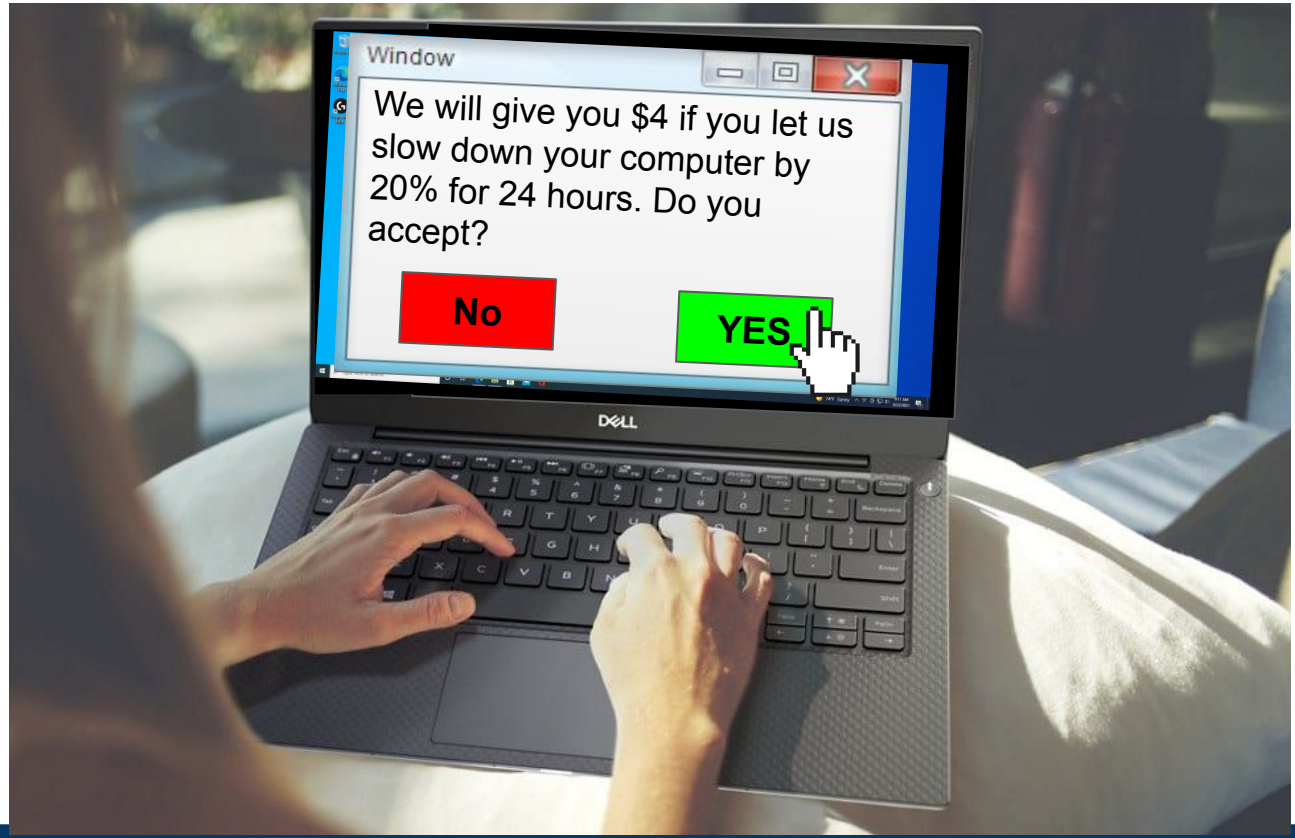
Experimental Protocol



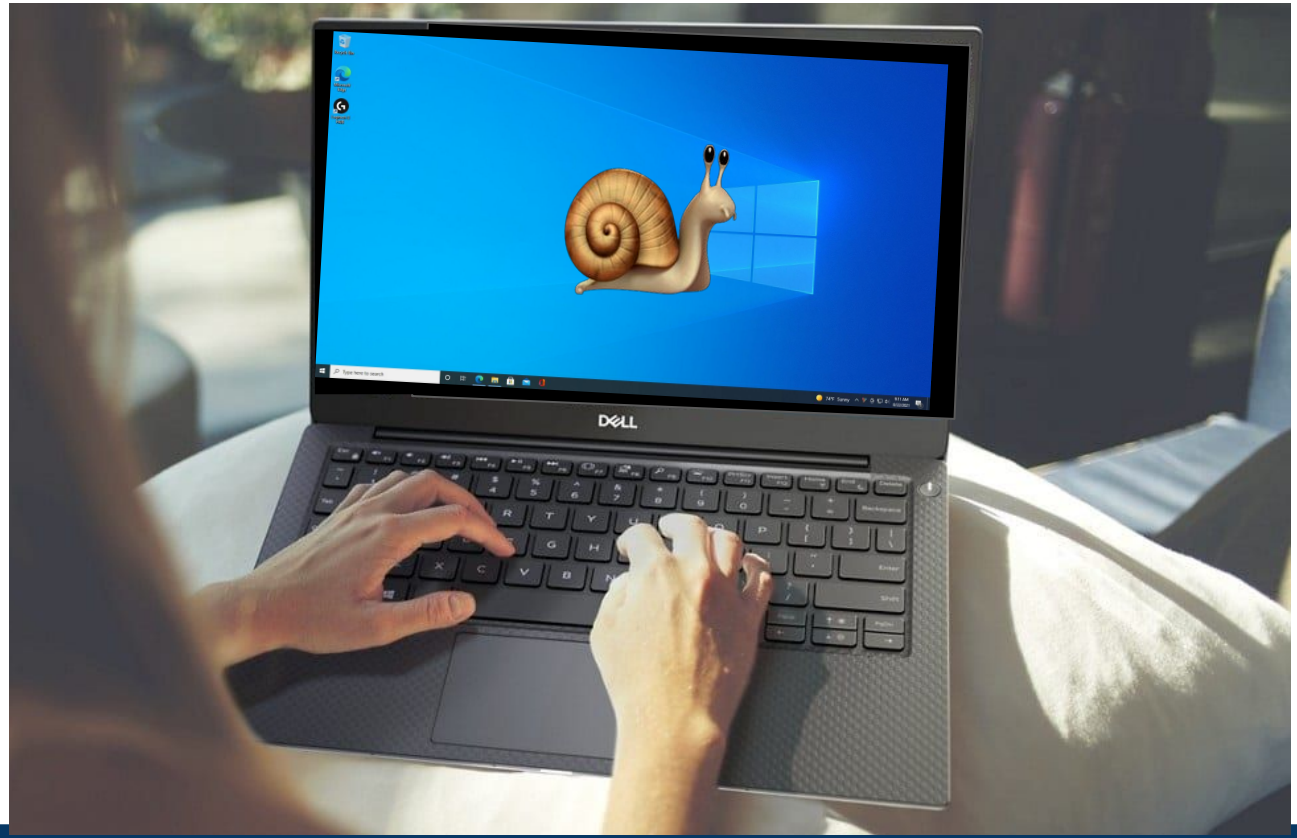
Experimental Protocol



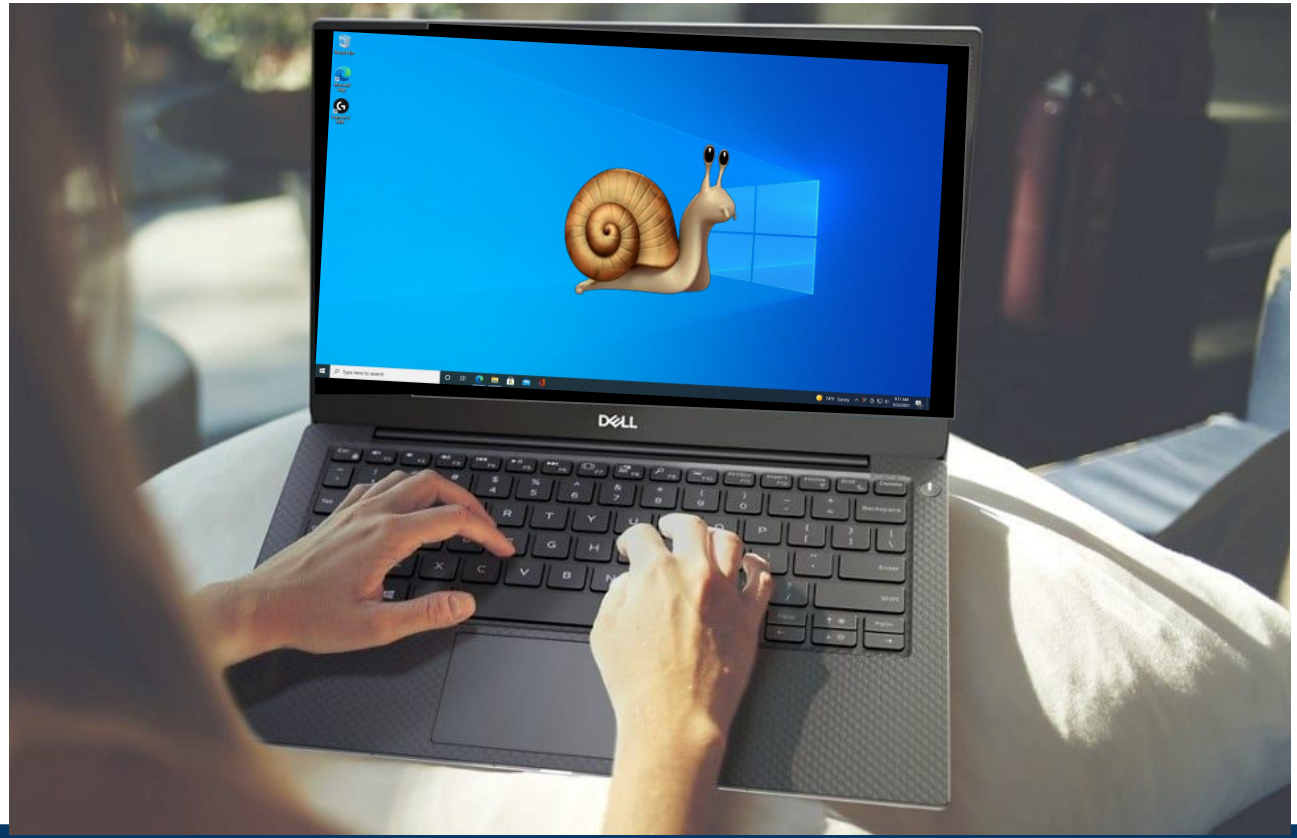
Experimental Protocol



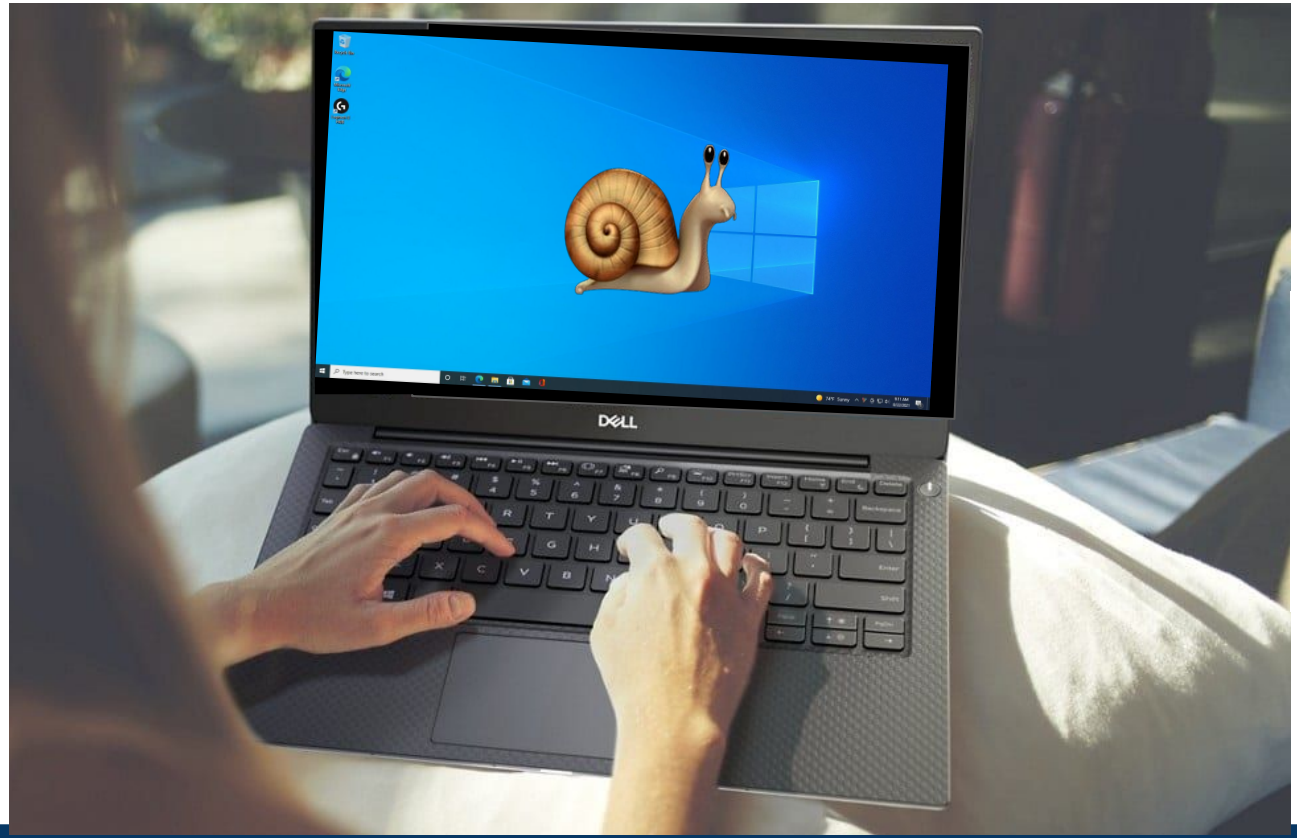
Experimental Protocol



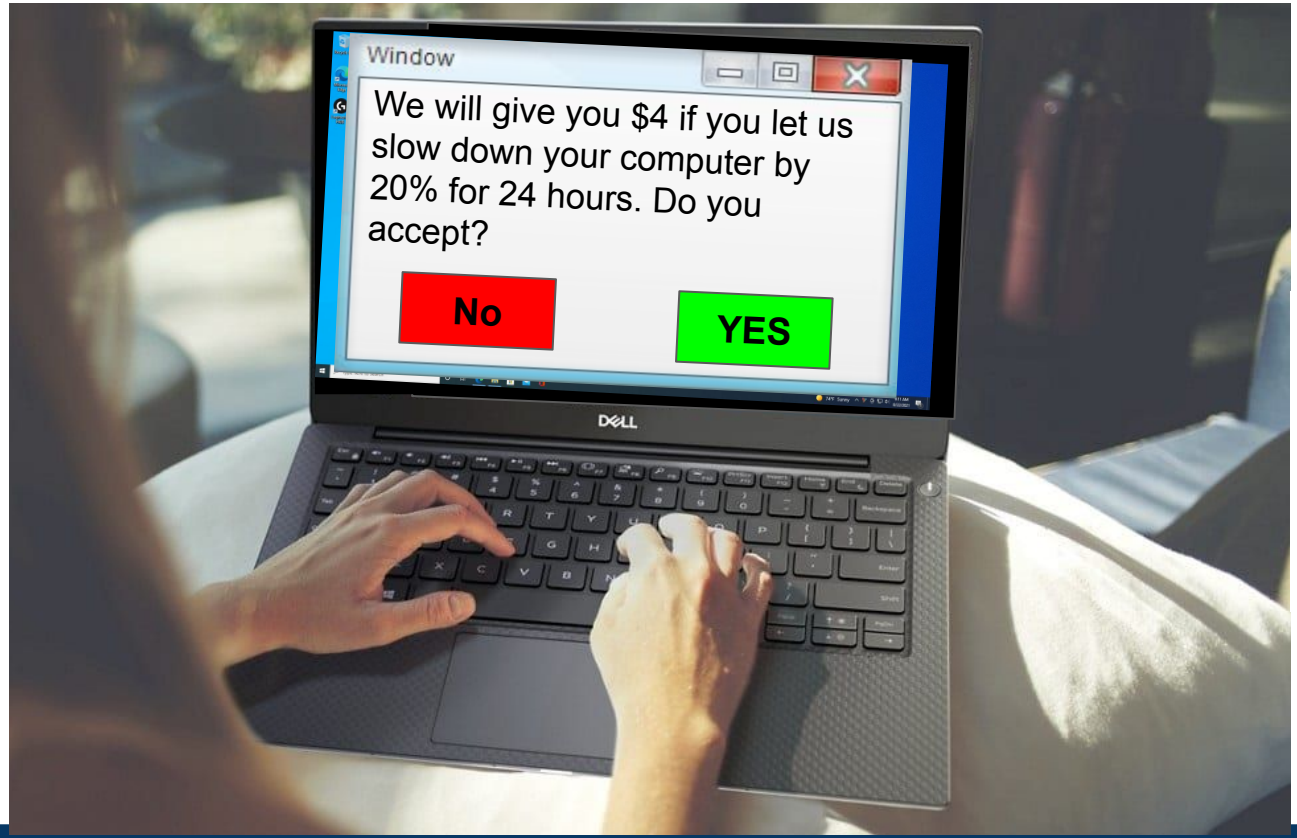
Experimental Protocol



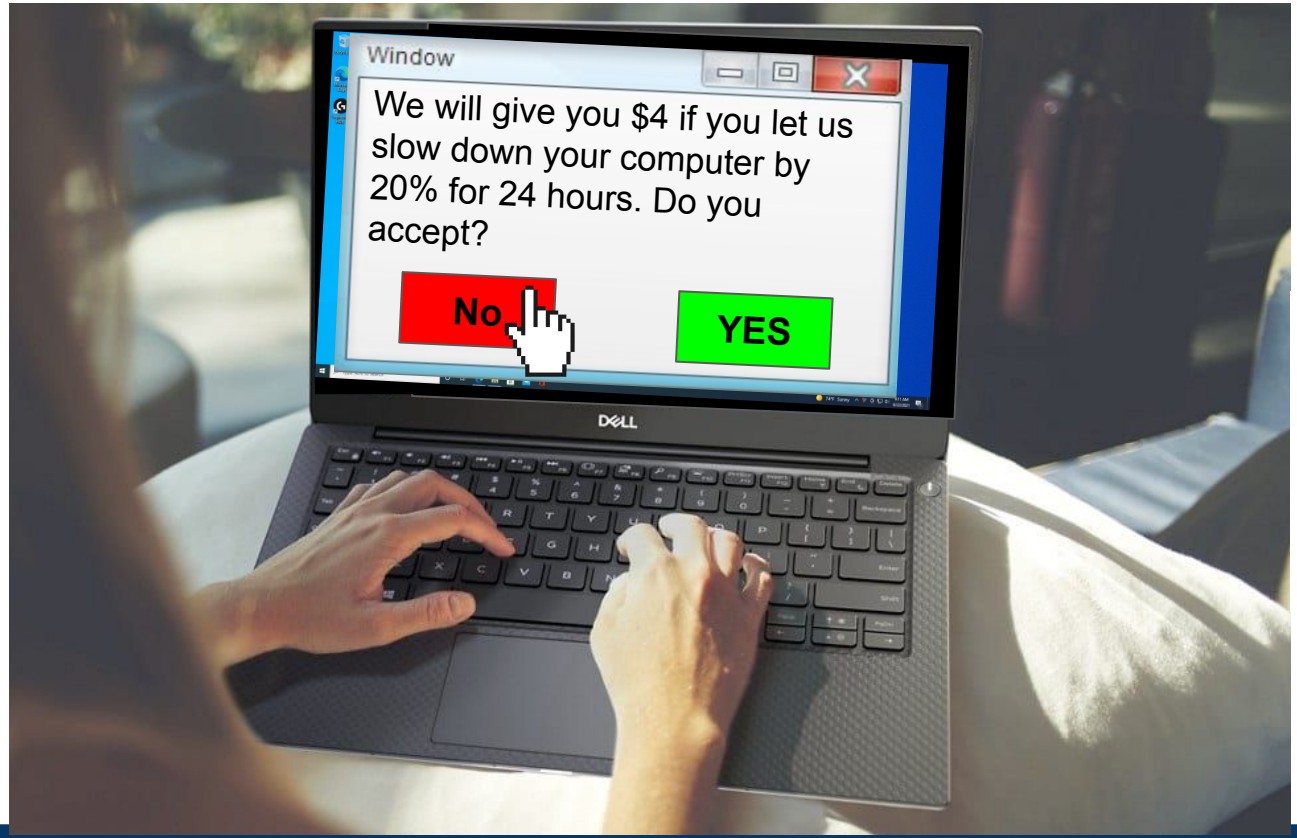
Experimental Protocol



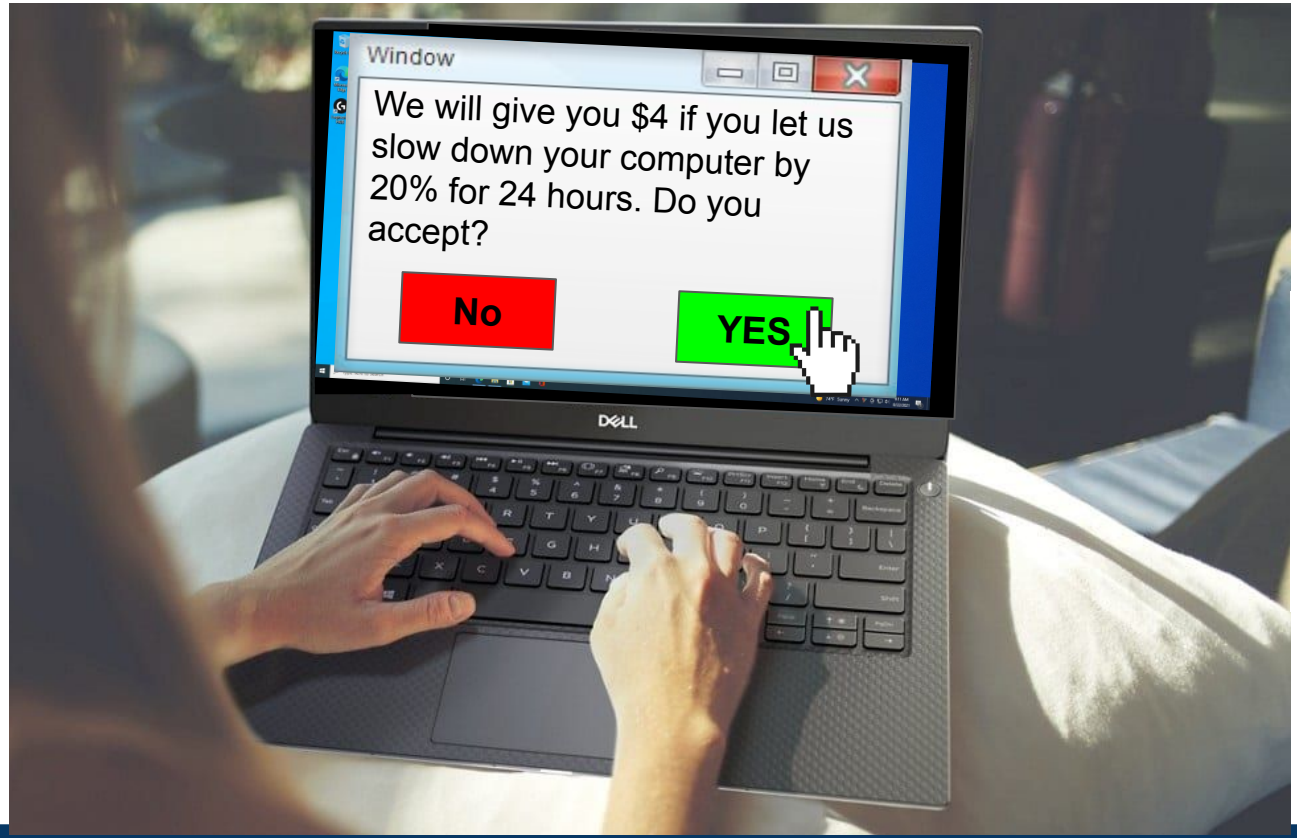
Experimental Protocol



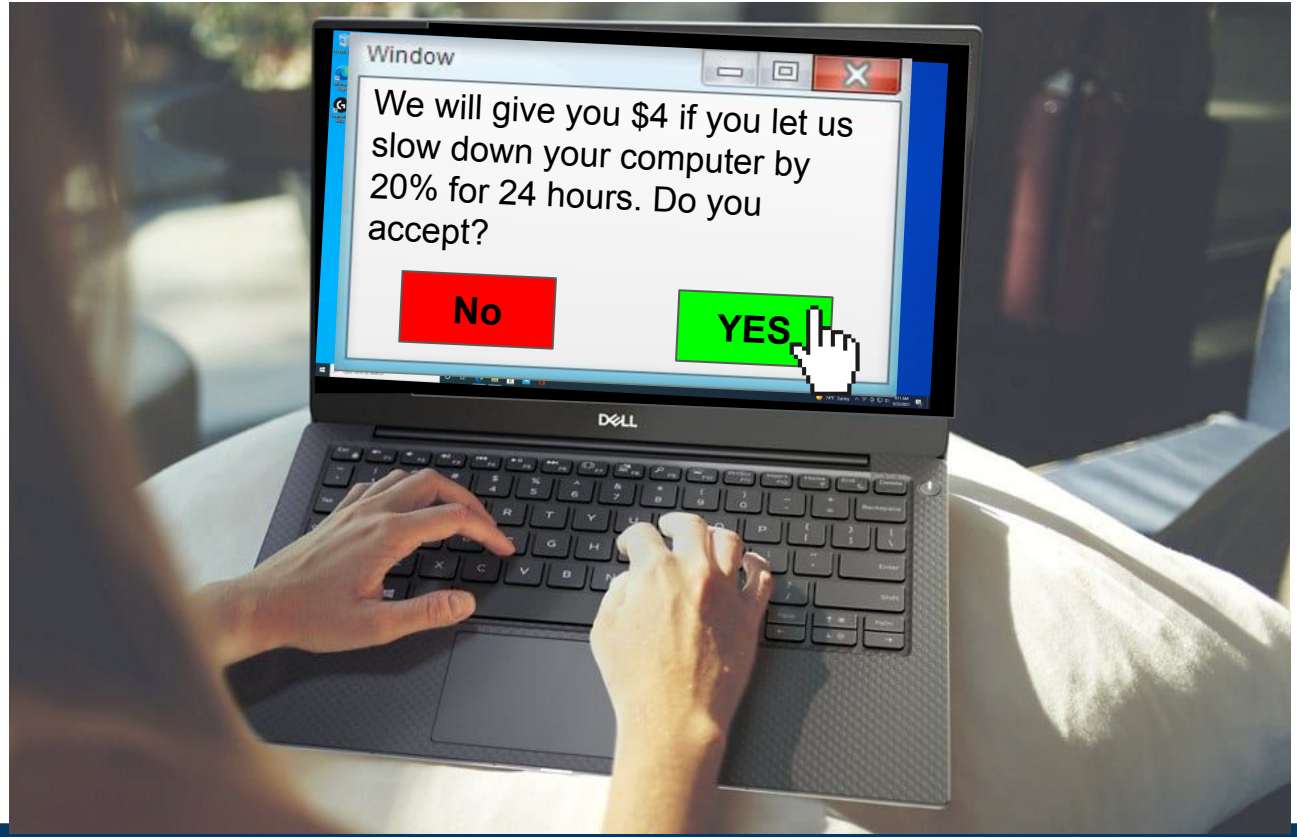
Experimental Protocol

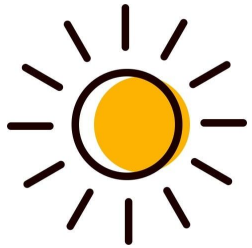


Experimental Protocol



Experimental Protocol





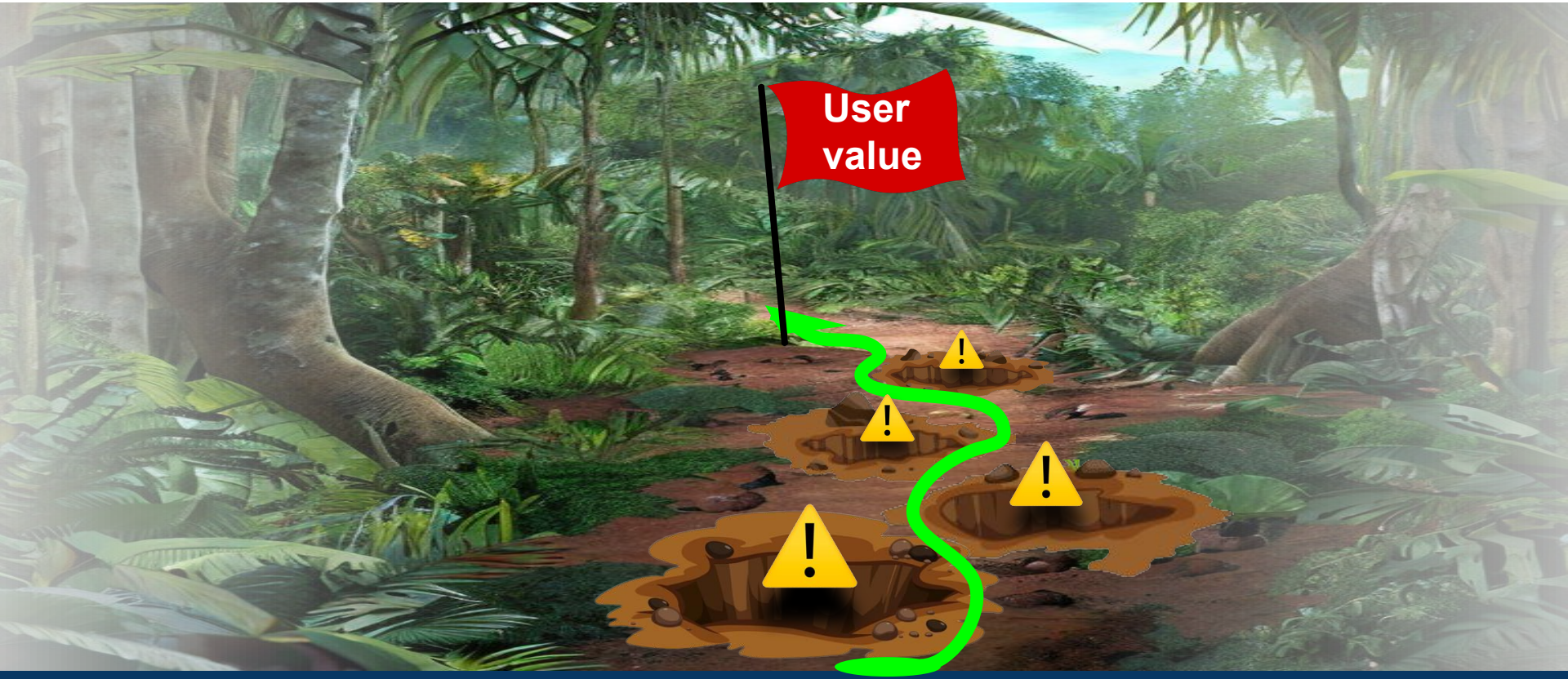
7x

Data Cleaning

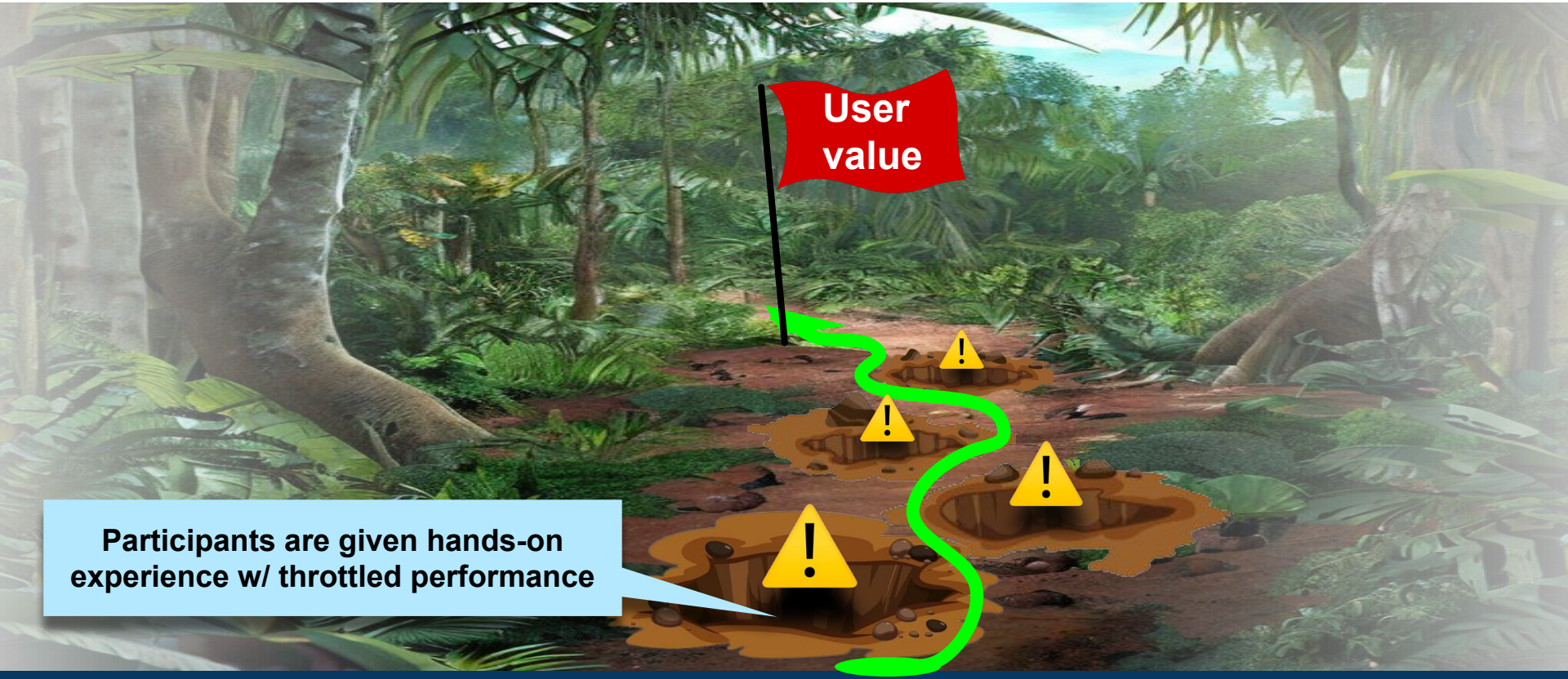
- What if they declined offer because…
  - They don’t trust us to modify device settings?
  - They share their device with a family member?
- What if they tried to “cheat”
  - by manually overriding the performance throttling?
  - by installing program on an unused machine?

After data cleaning, all remaining participants decisions **based on dollar amount of offer price only**

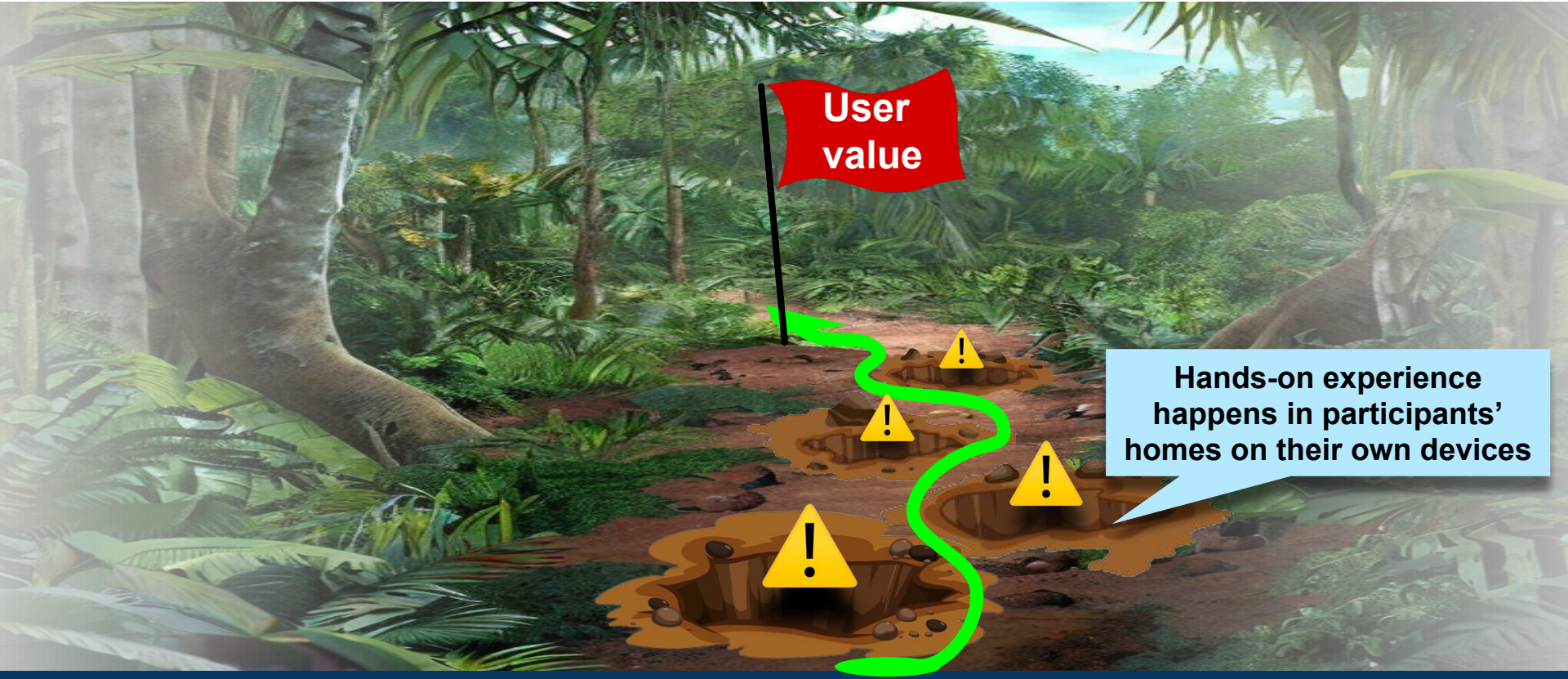
Our experimental protocol navigates the pitfalls!



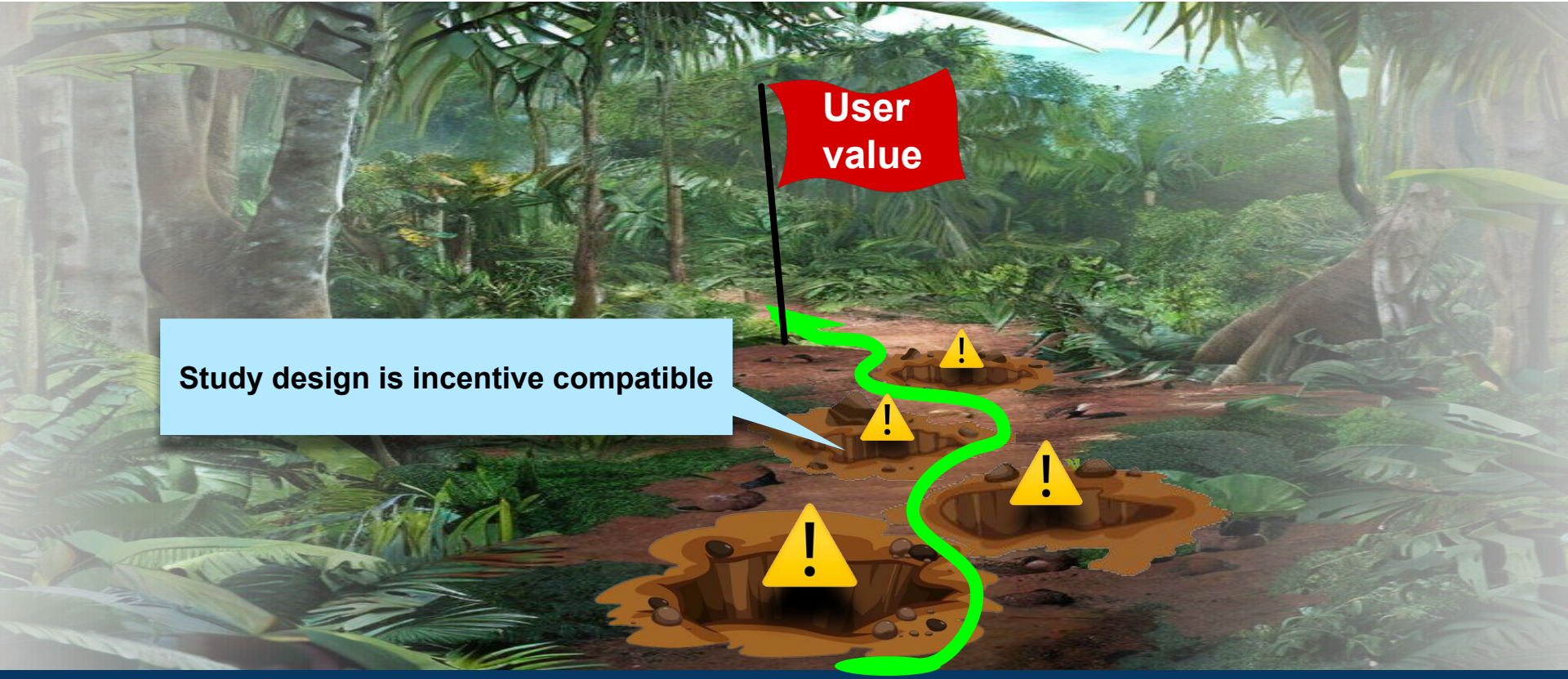
Our experimental protocol navigates the pitfalls!



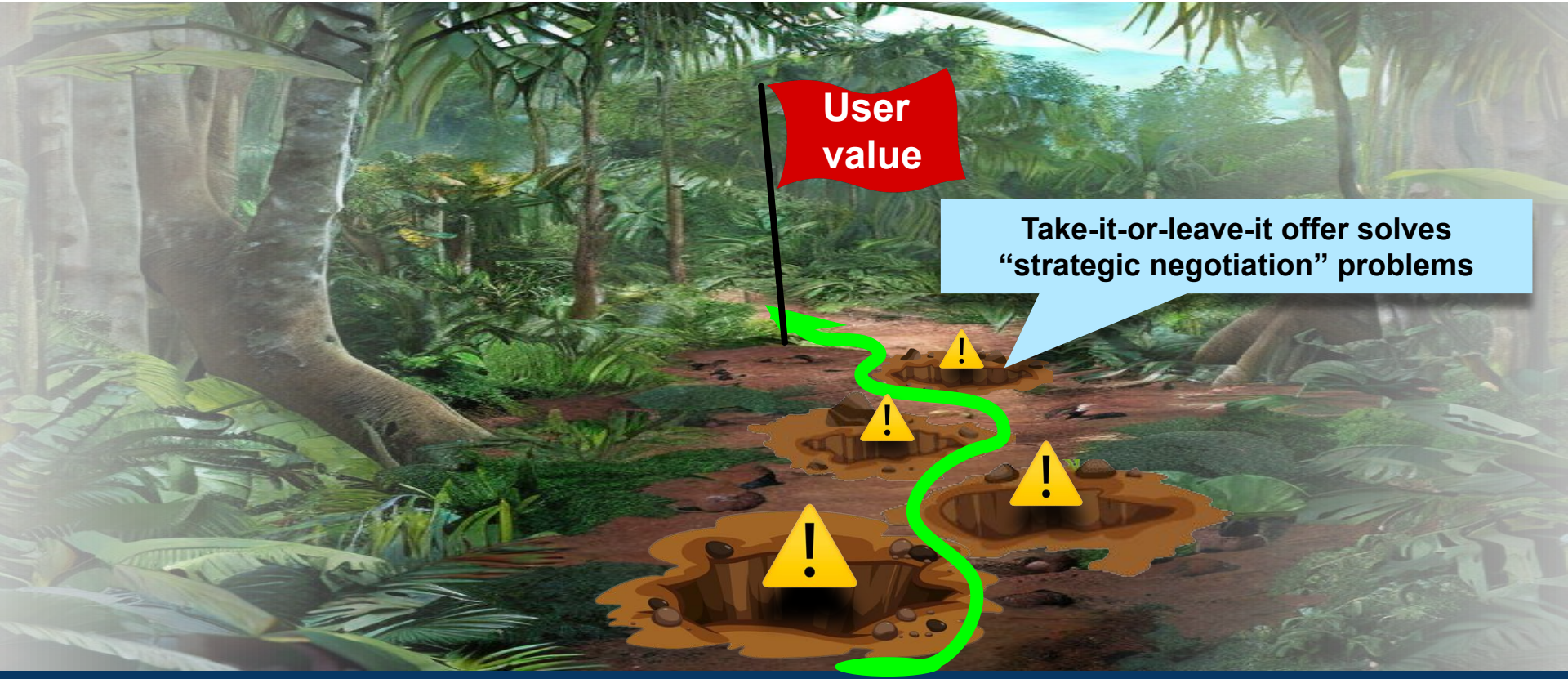
Our experimental protocol navigates the pitfalls!



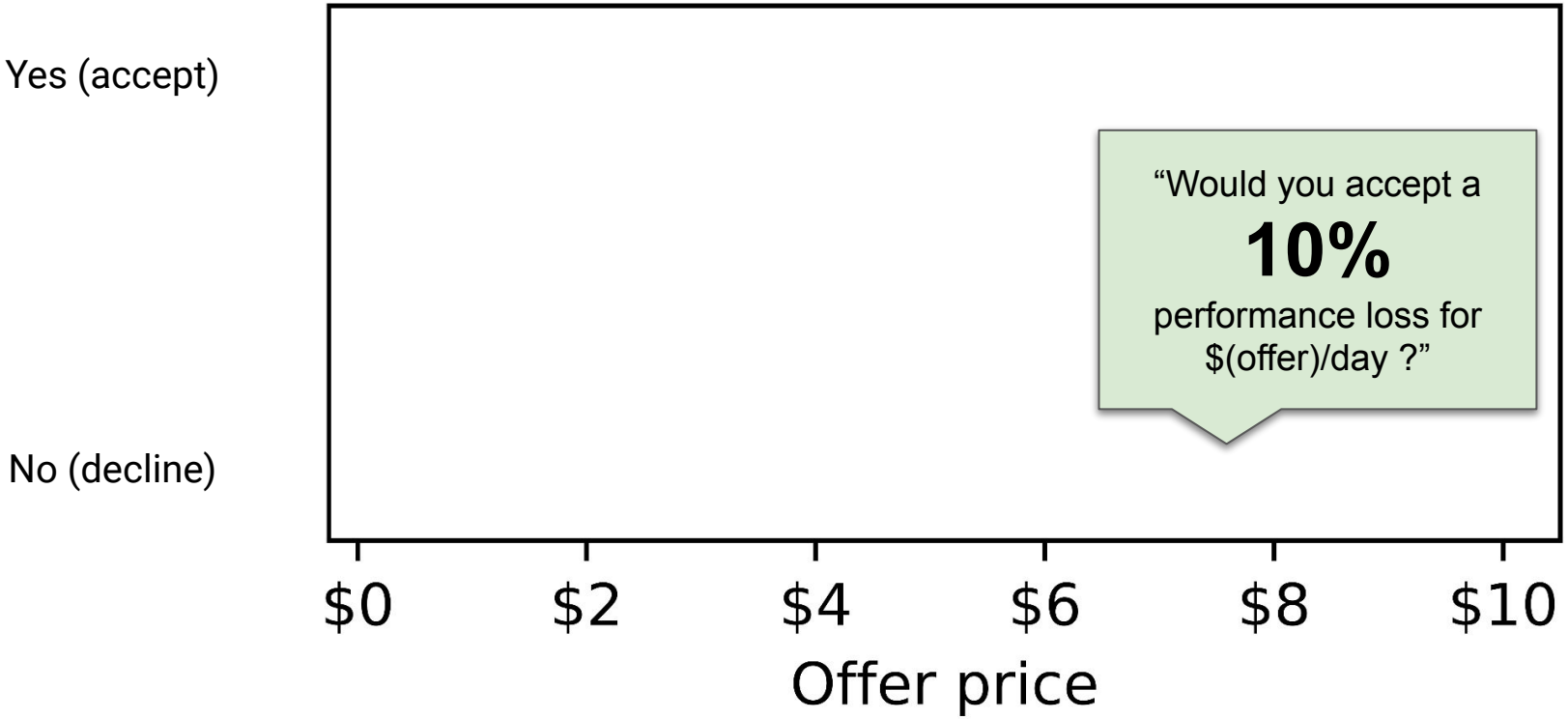
Our experimental protocol navigates the pitfalls!



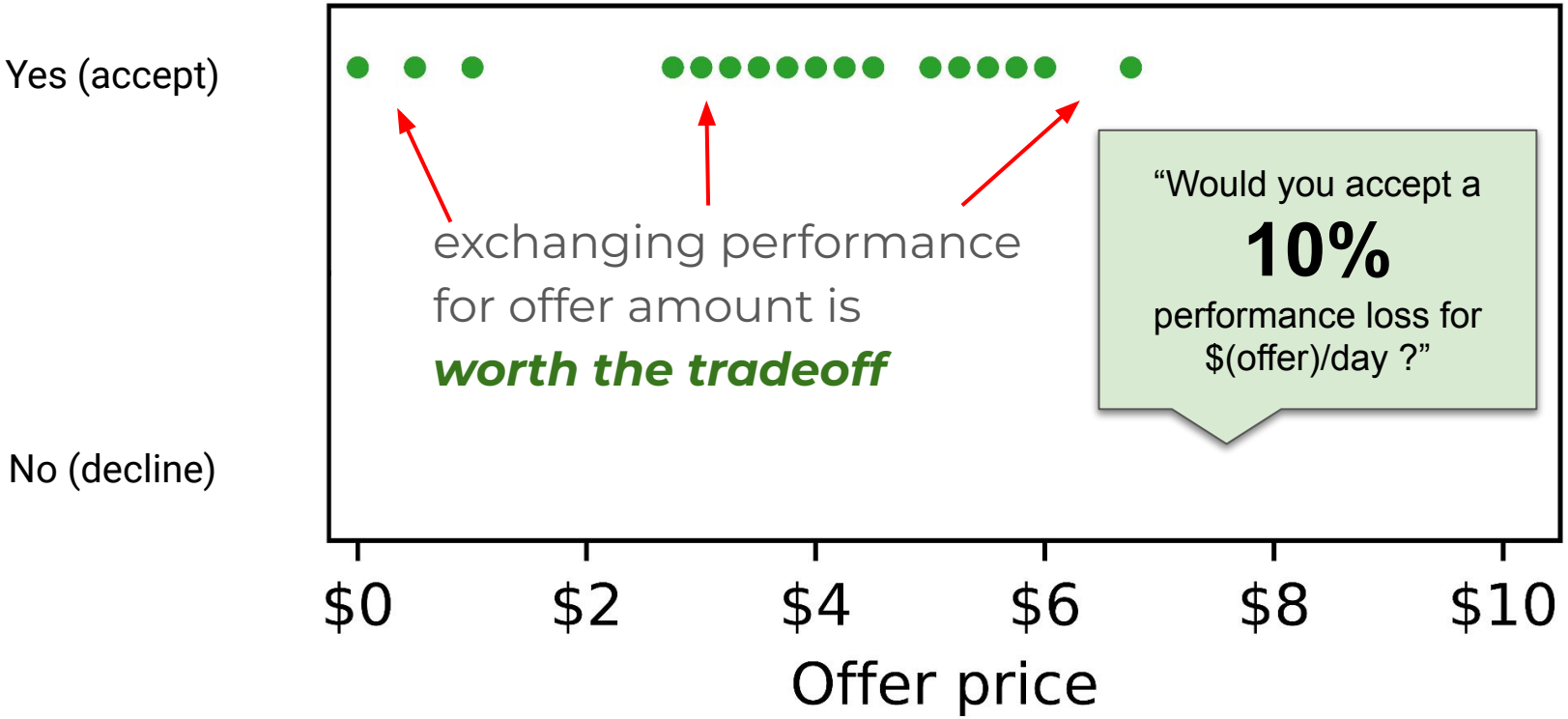
Our experimental protocol navigates the pitfalls!



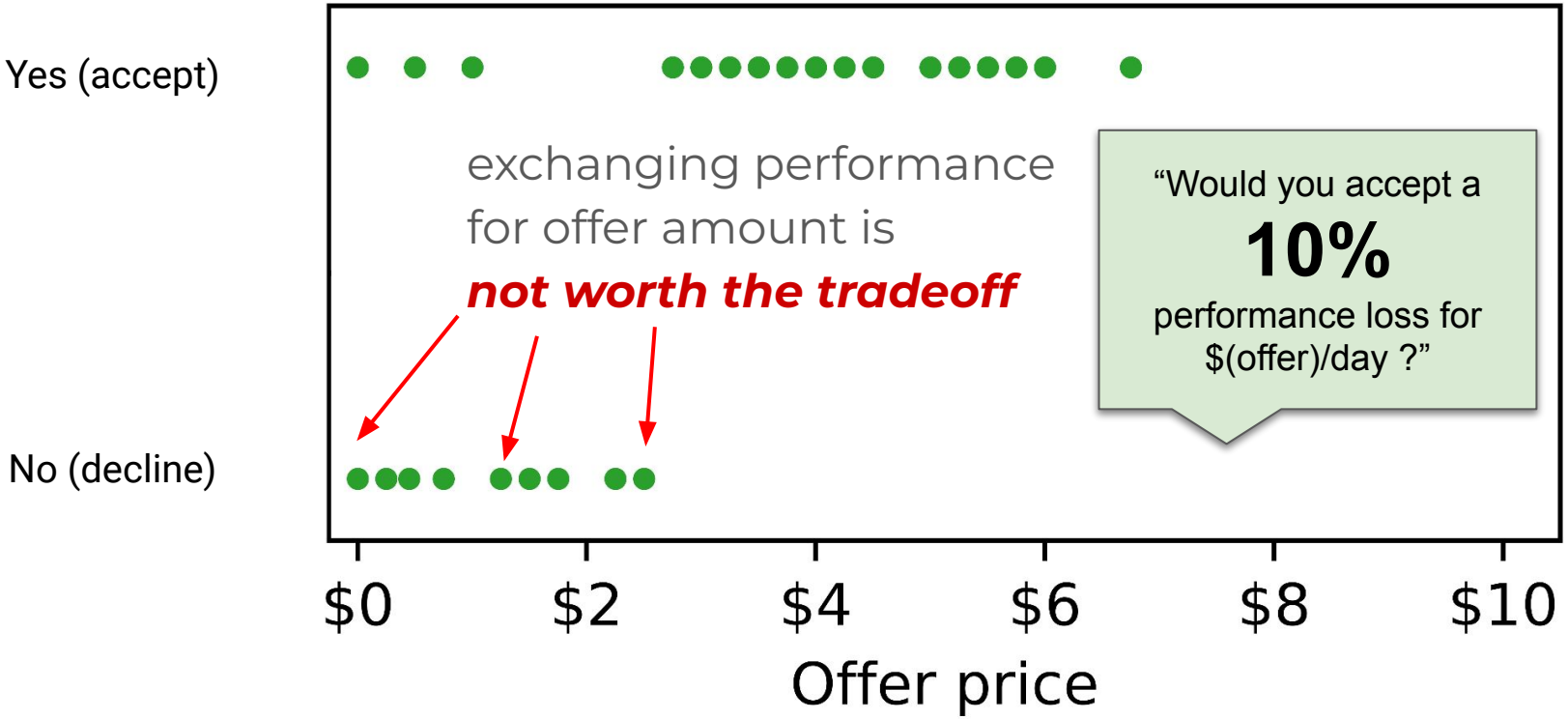
Study Results



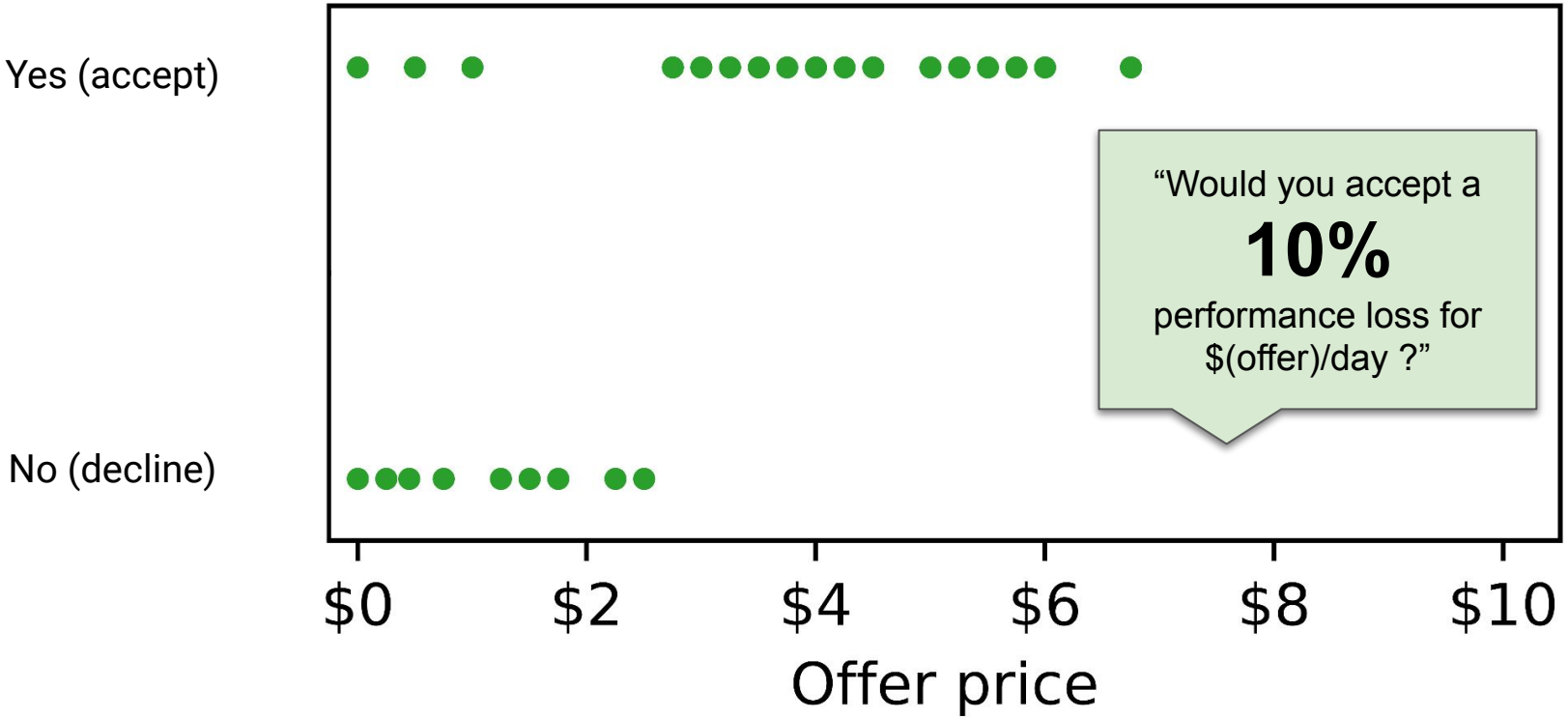
Study Results



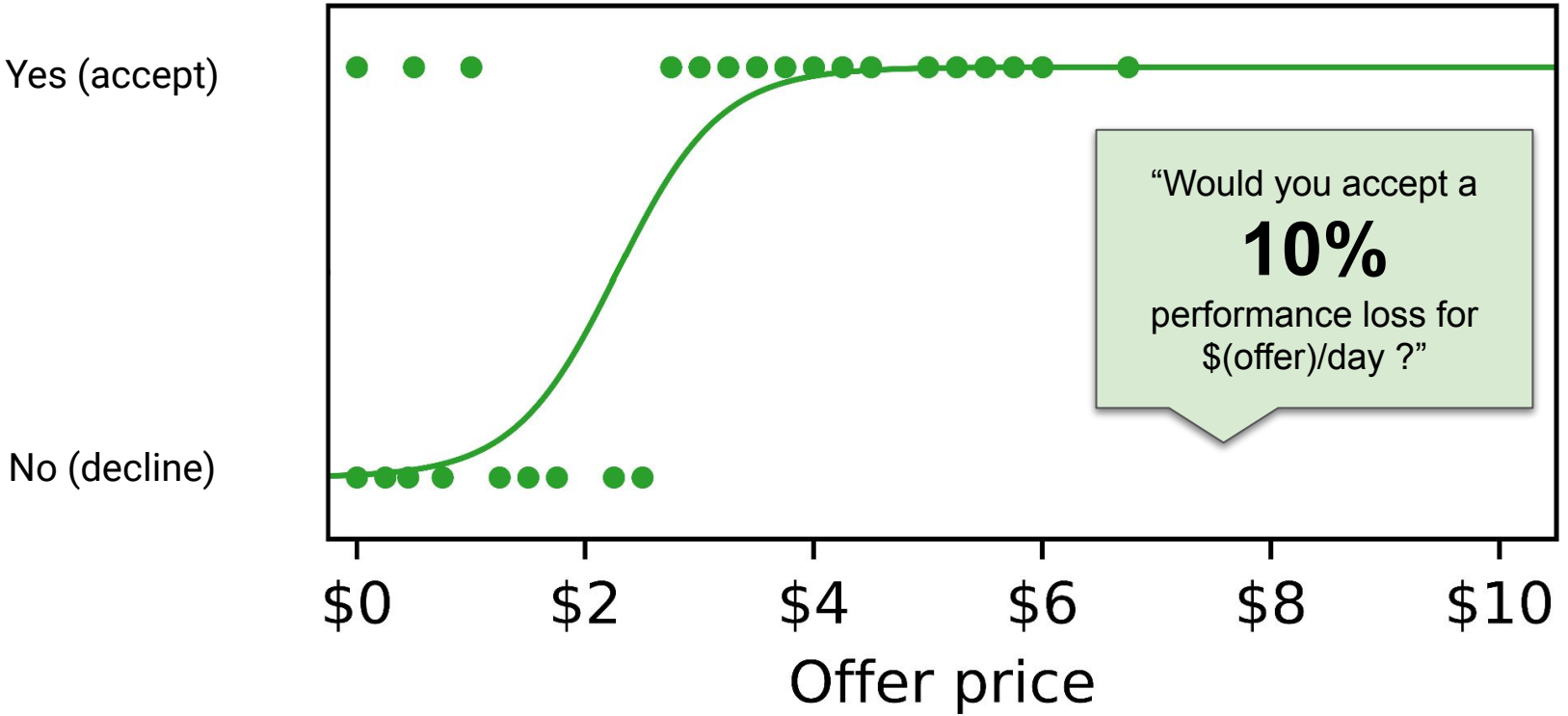
Study Results



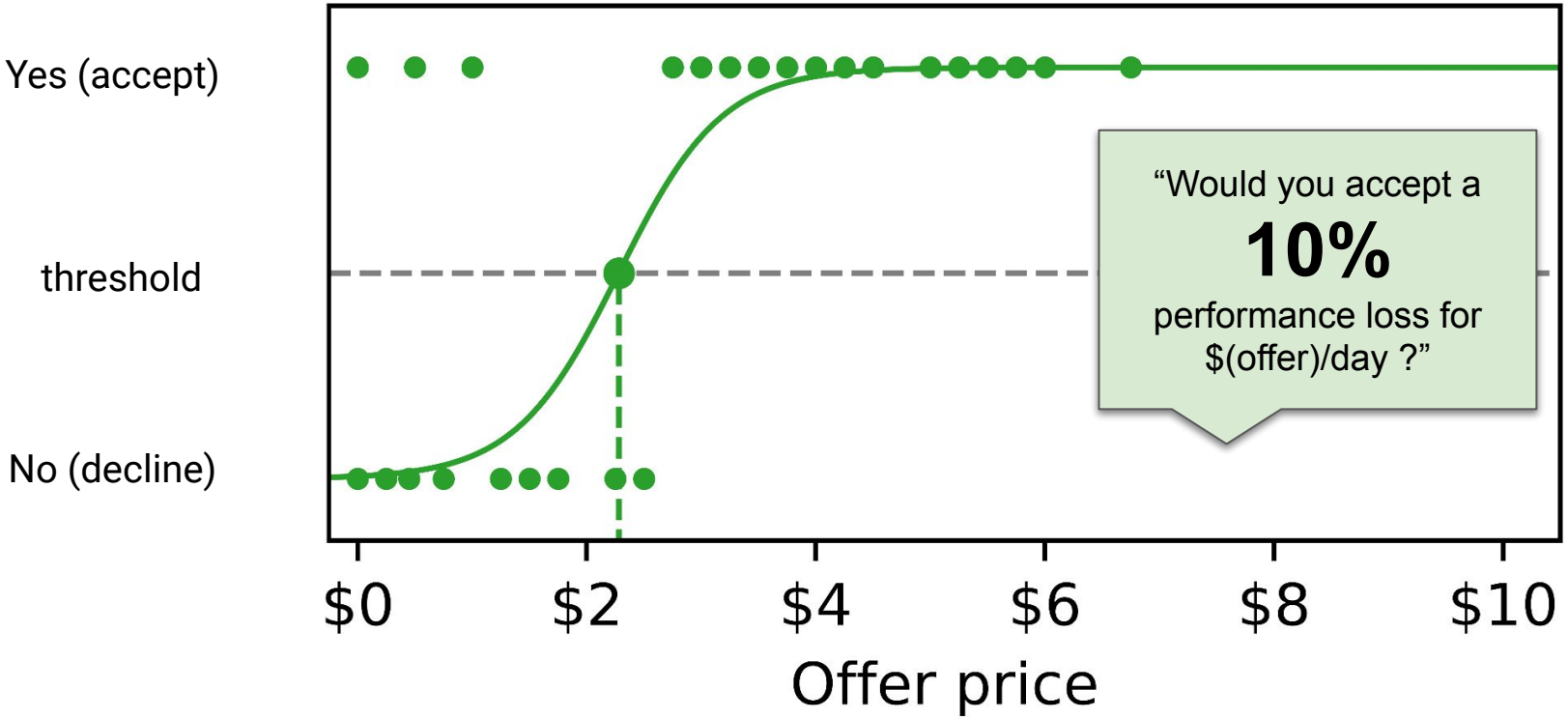
Study Results



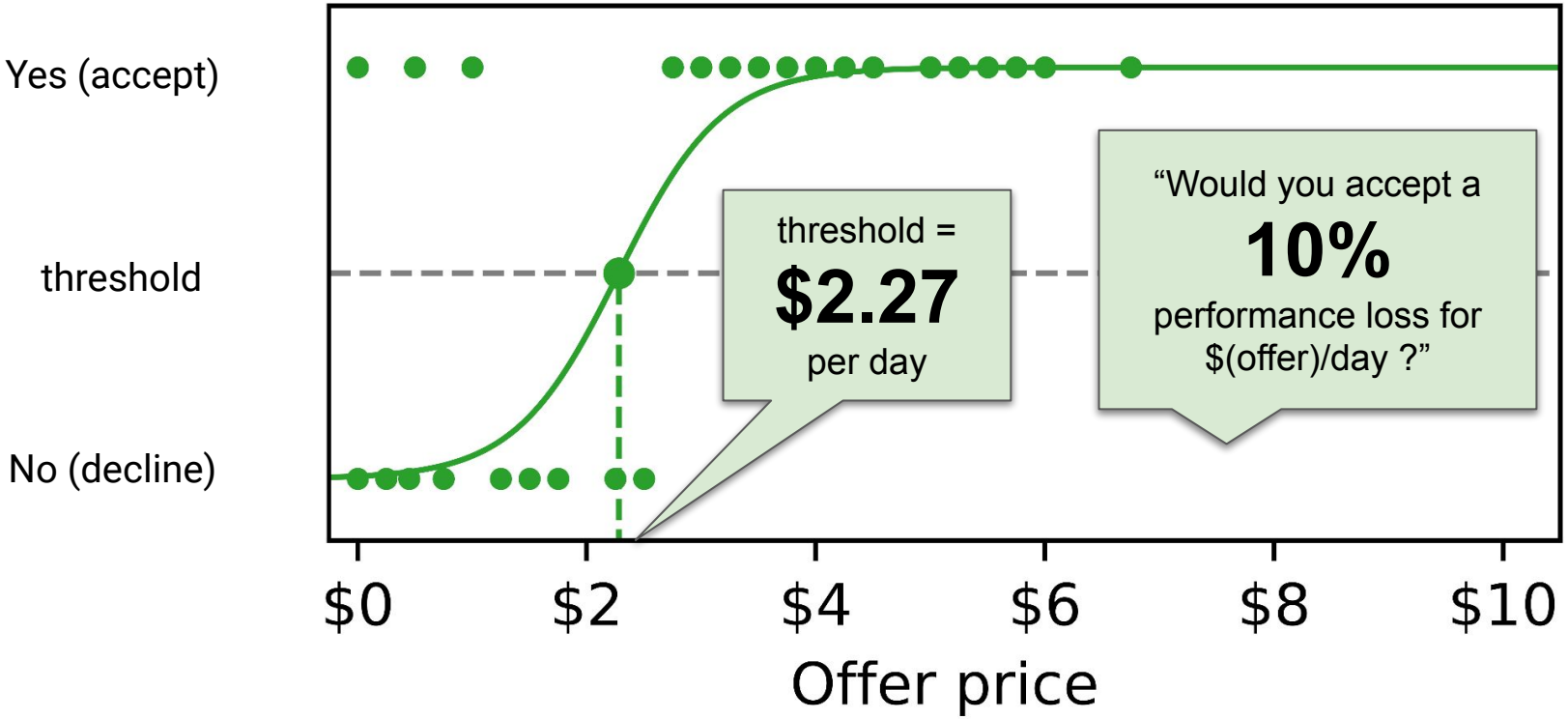
Study Results



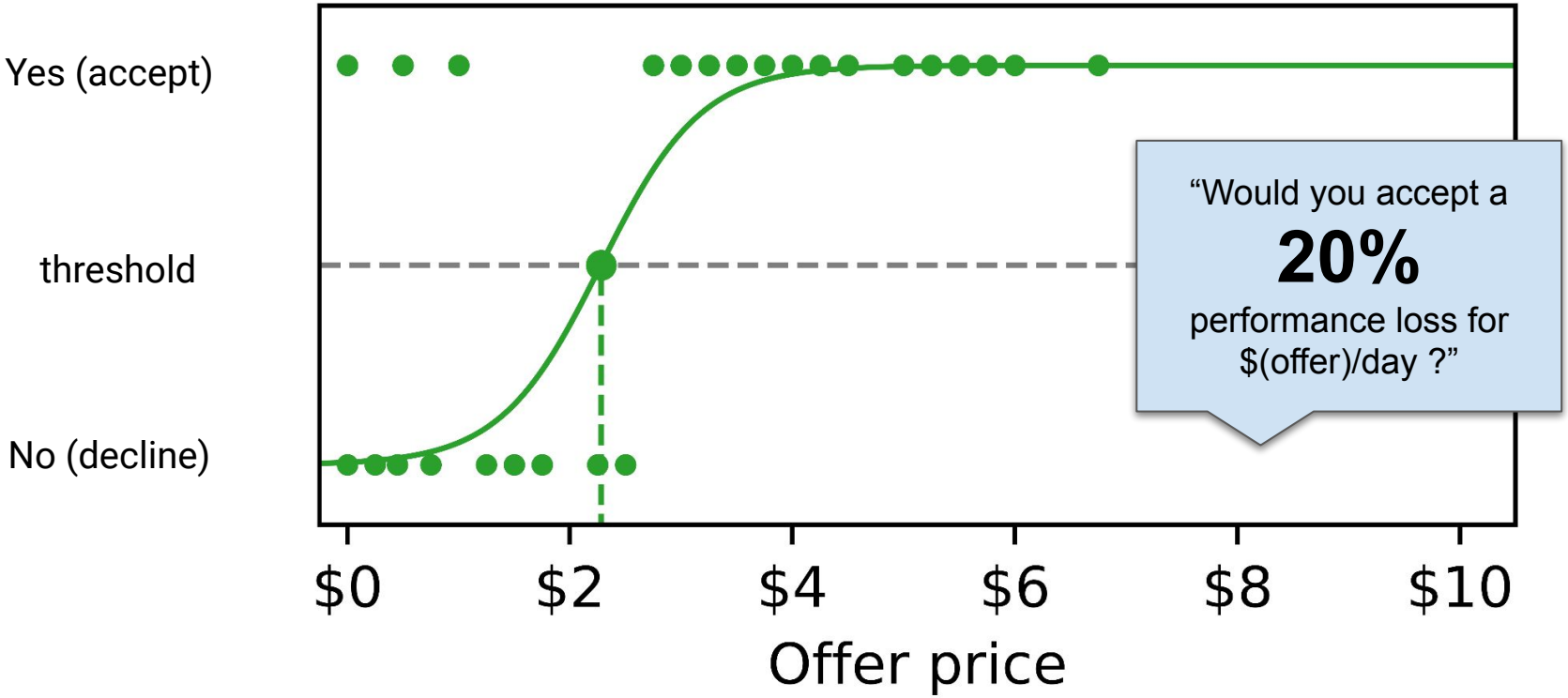
Study Results



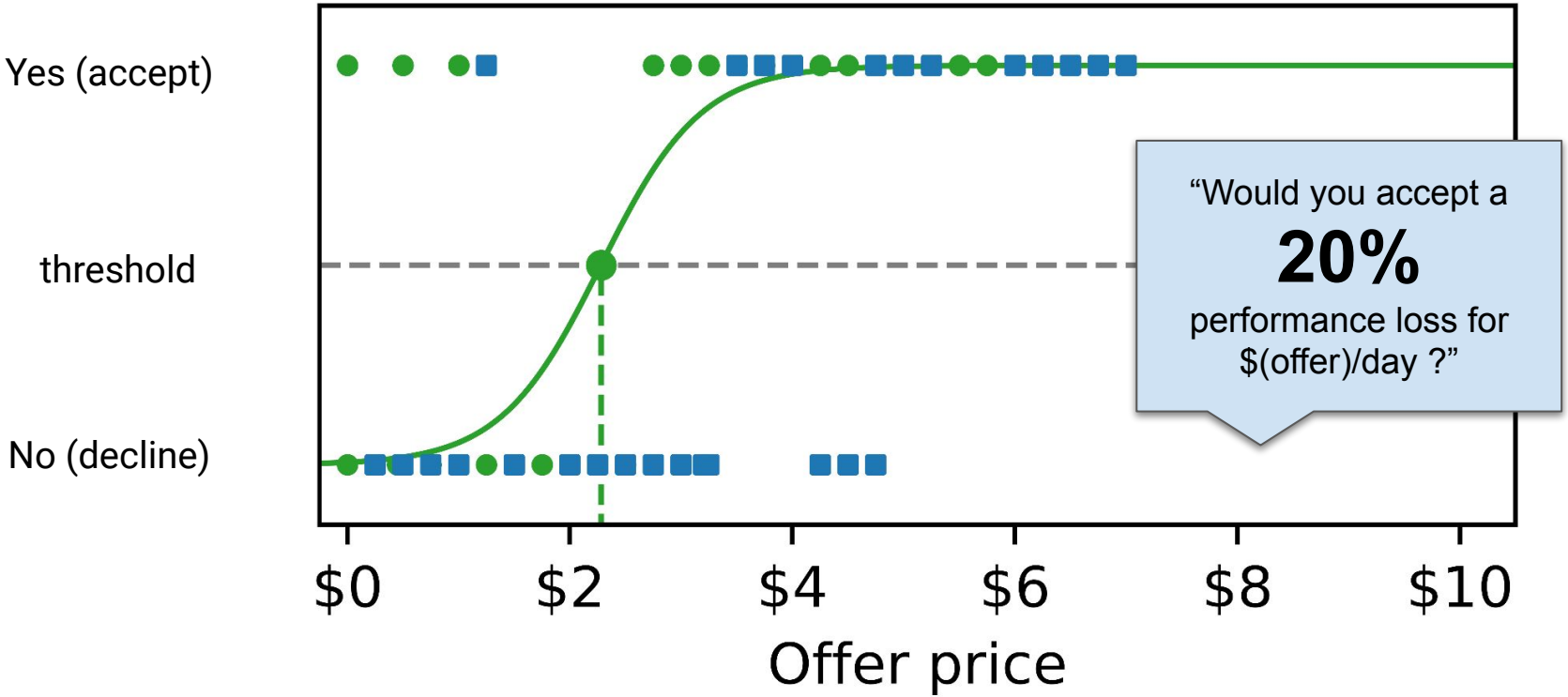
Study Results



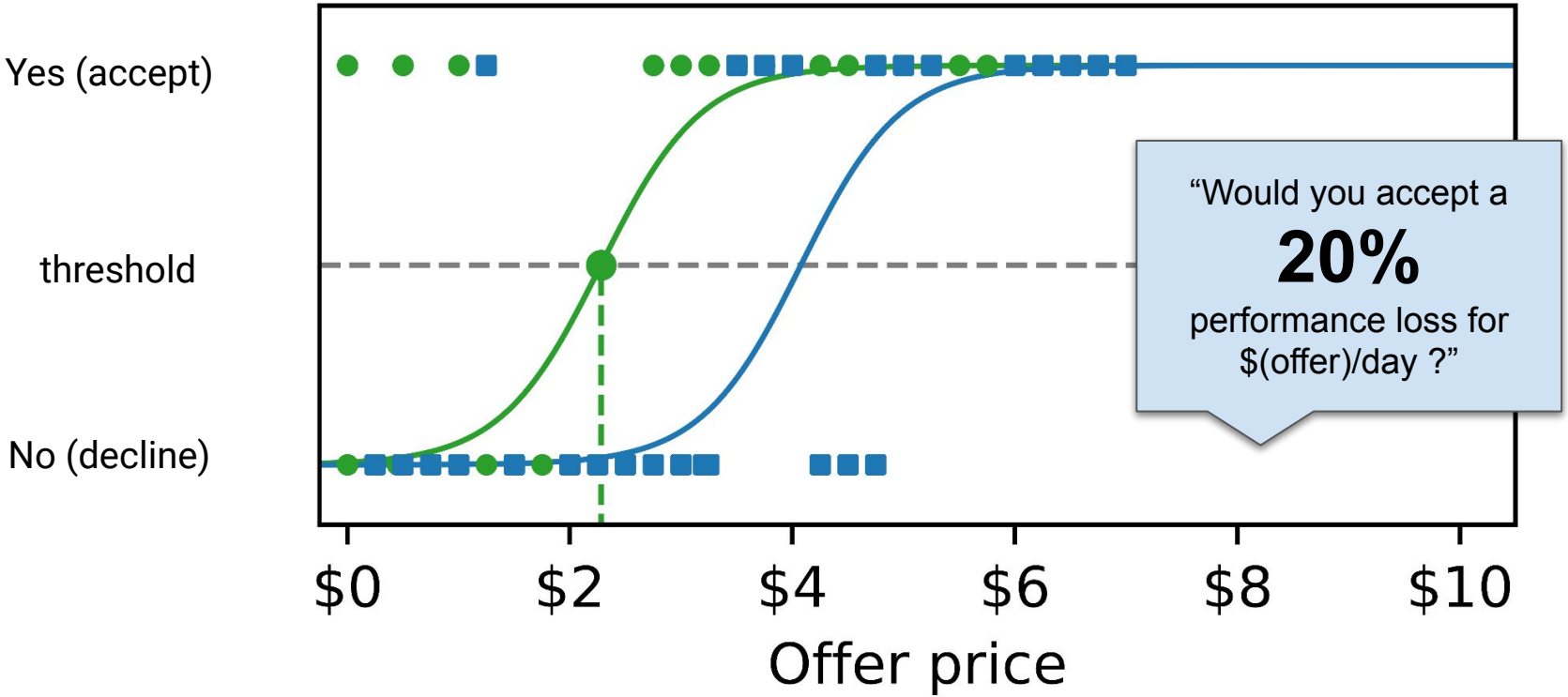
Study Results



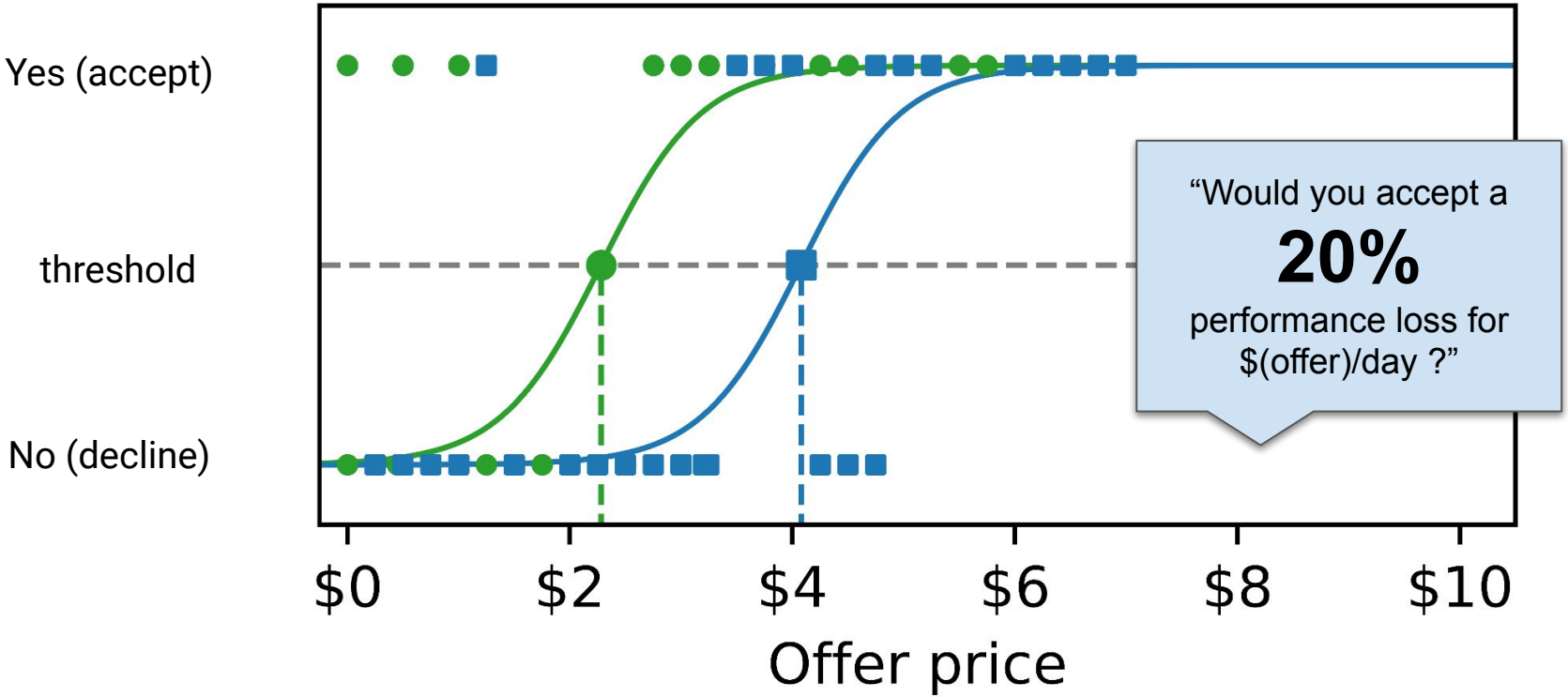
Study Results



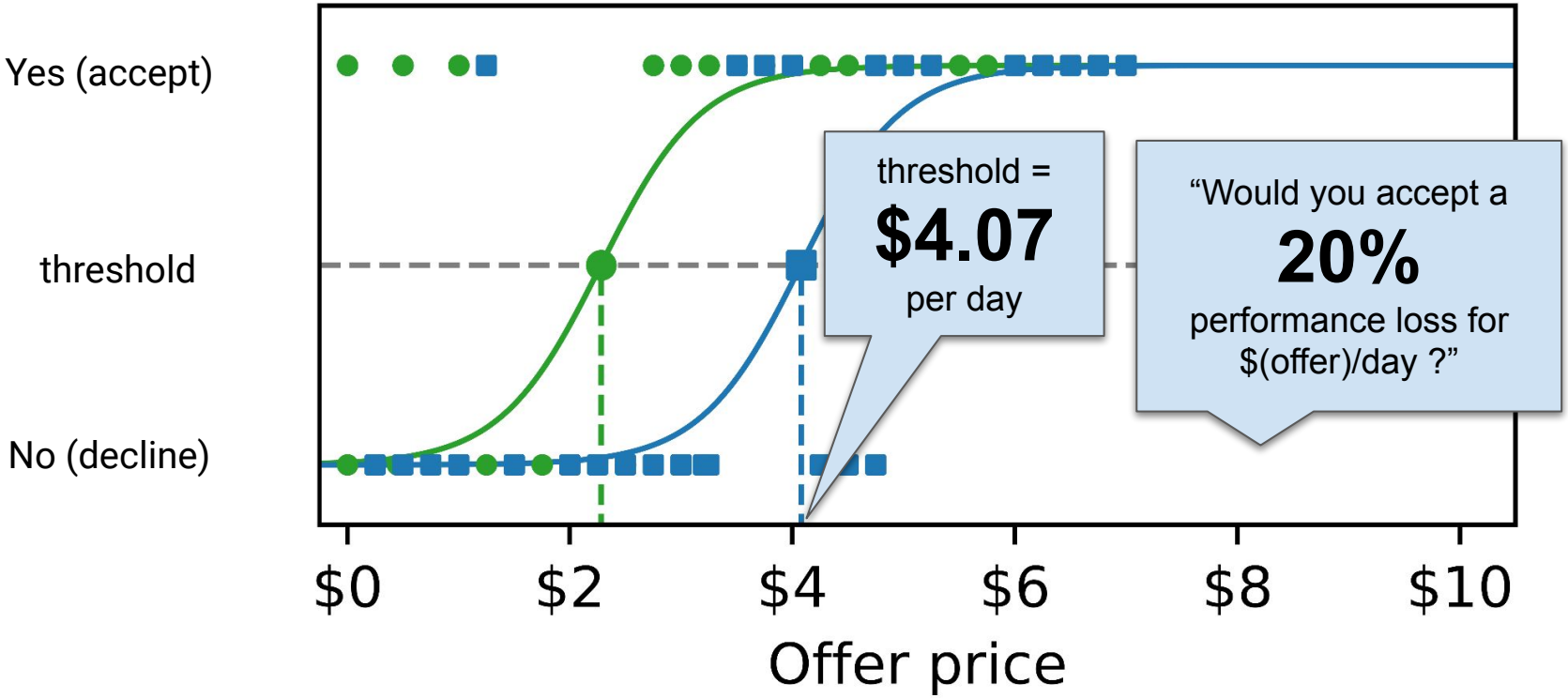
Study Results



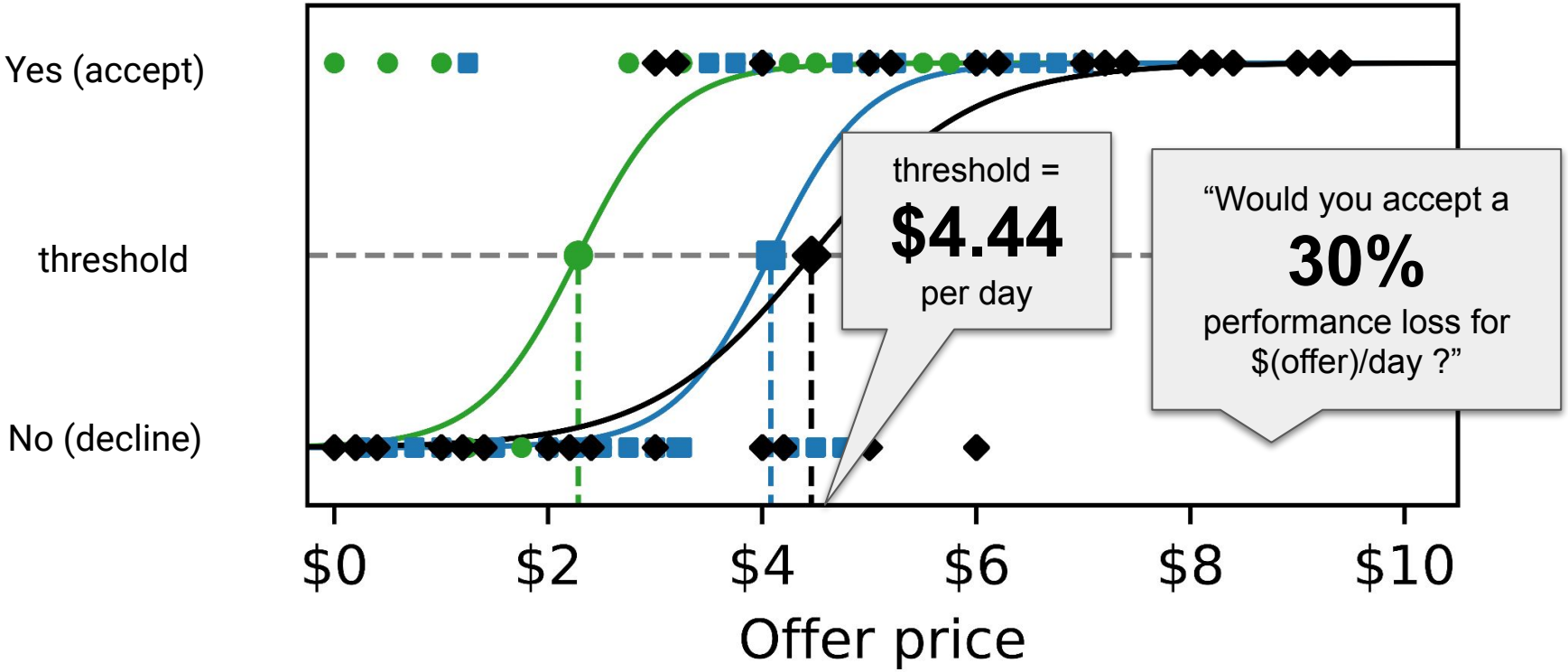
Study Results



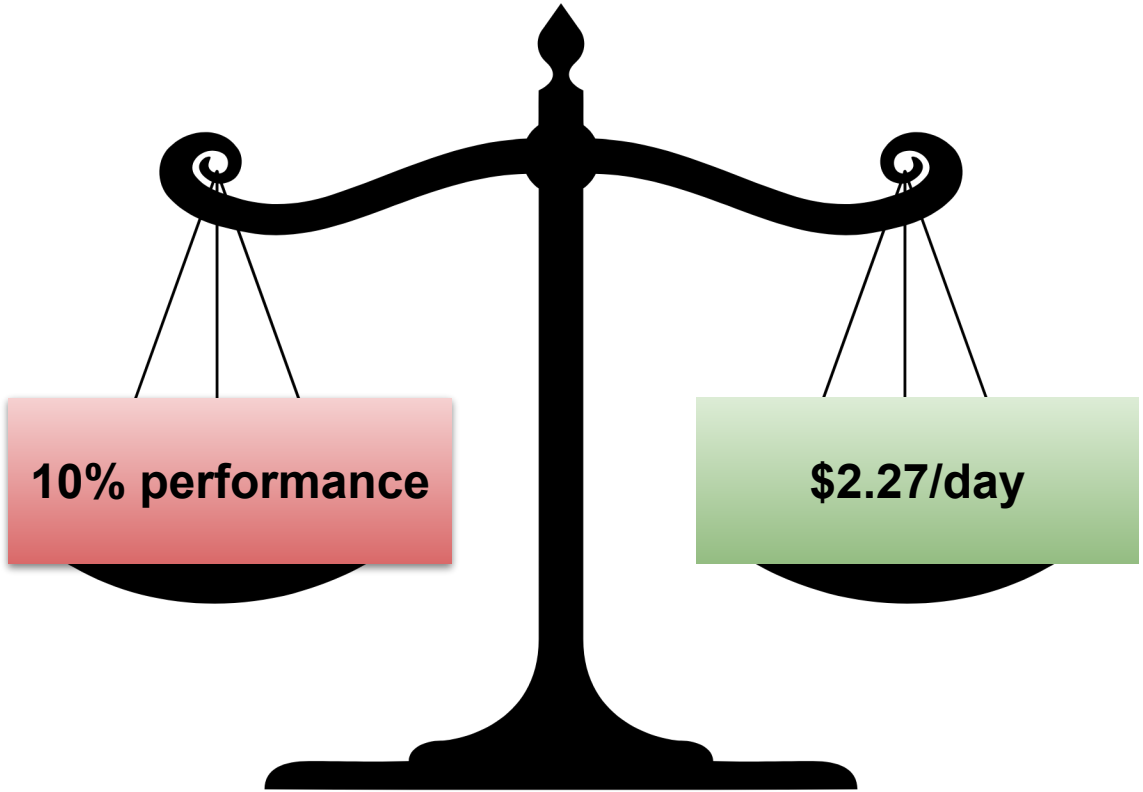
Study Results



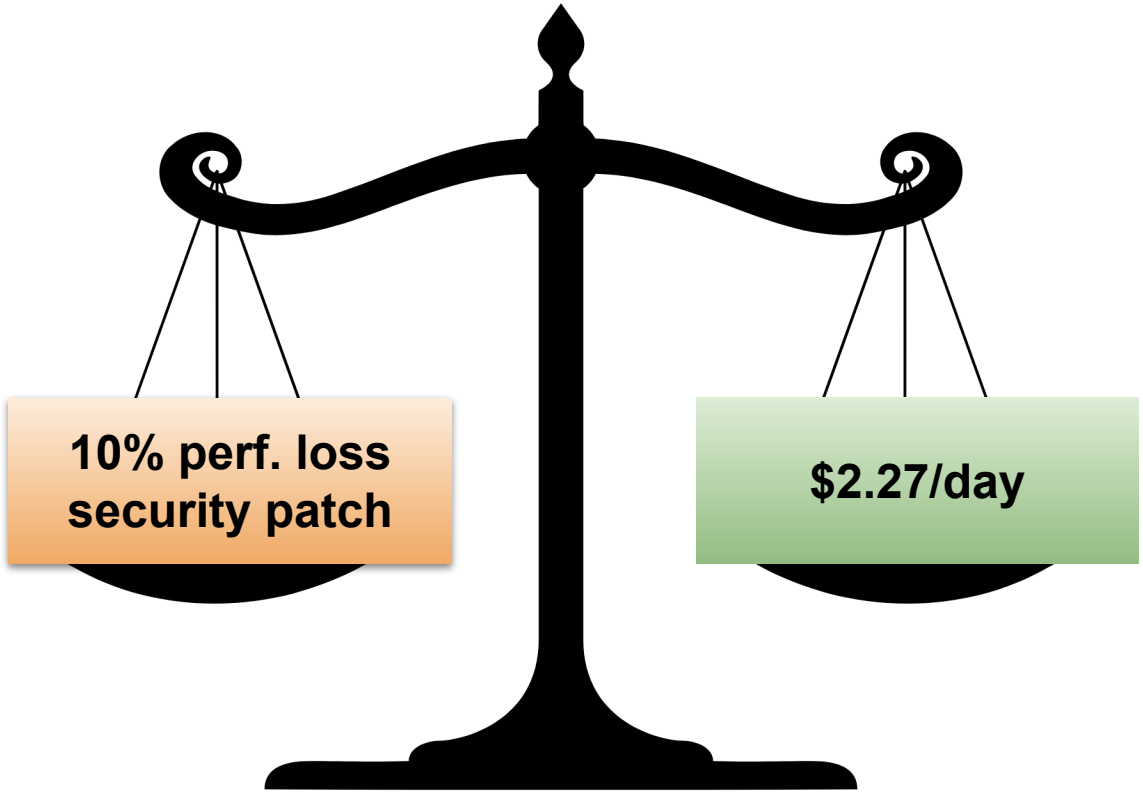
Study Results



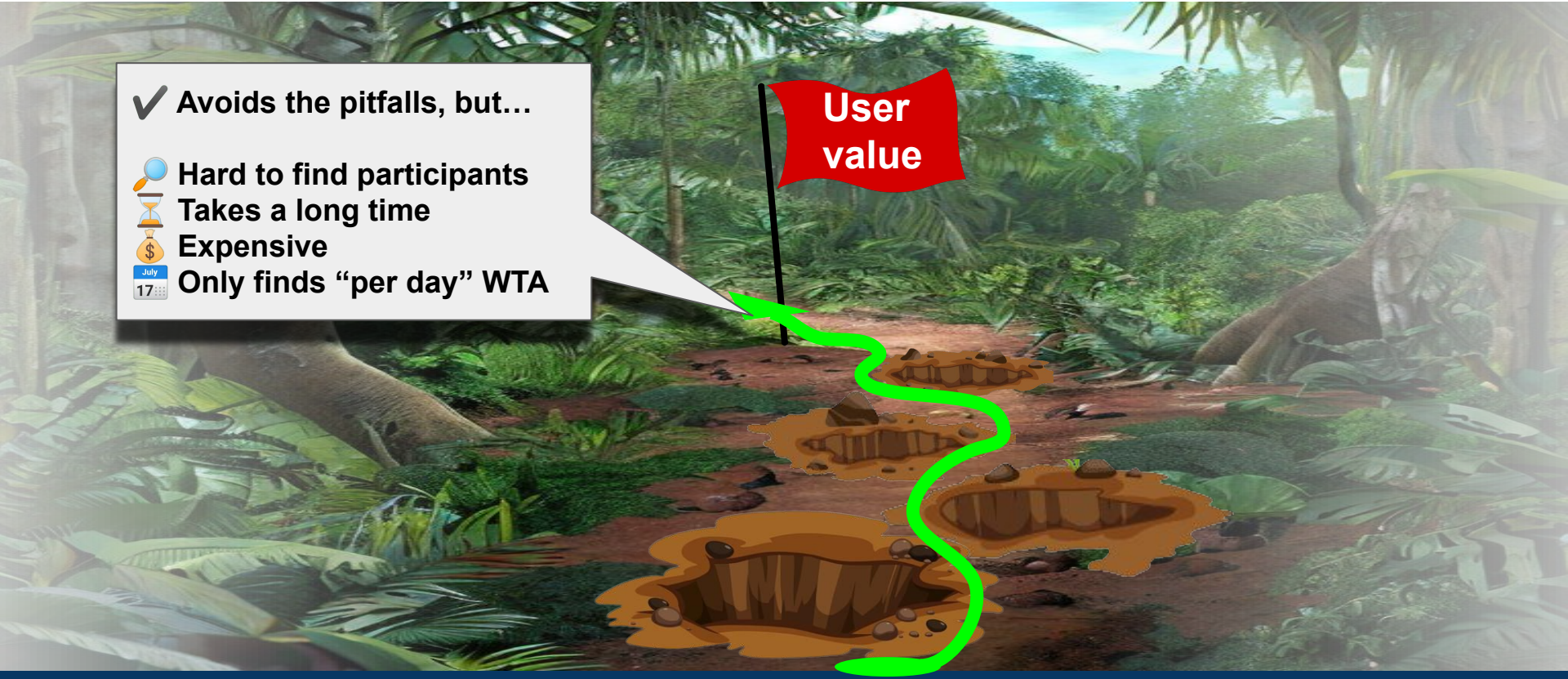
Goal: Find “exchange rate” between performance and user value



Goal: Find “exchange rate” between performance and user value



Drawbacks


✔ Avoids the pitfalls, but…
Hard to find participants
Takes a long time
Expensive
Only finds “per day” WTA
User value

Three methods to find user value

Experiment #1:
Long-Term Incentive Compatible Study

Experiment #2:
Simple Survey

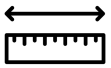
Experiment #3:
Guided Tasks-Based Study

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan



measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyberinsurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

modeling

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '23, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

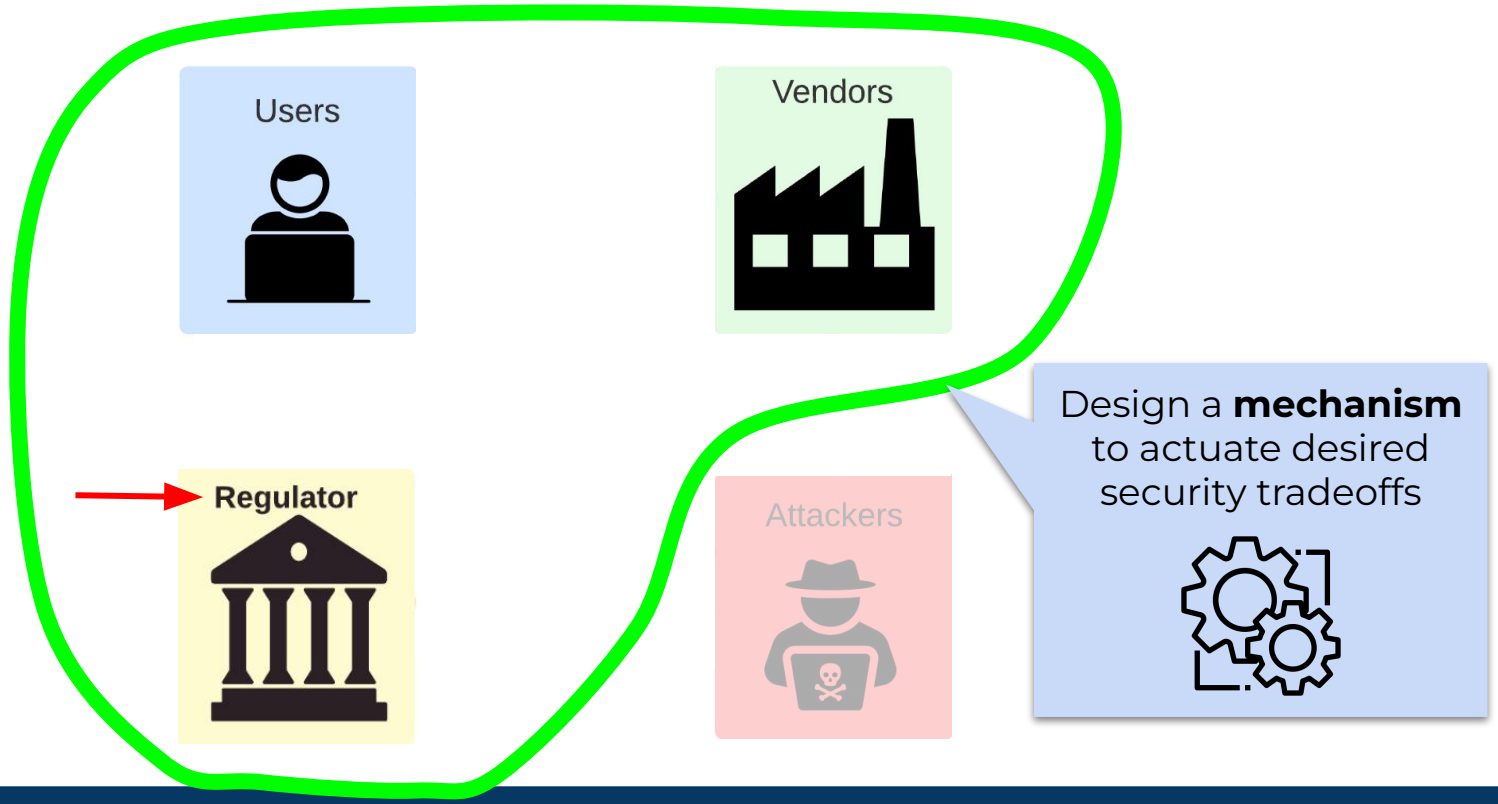
mechanisms

Simulations of Cyberinsurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

modeling

Architectural Security Regulation

Architectural Security Regulation

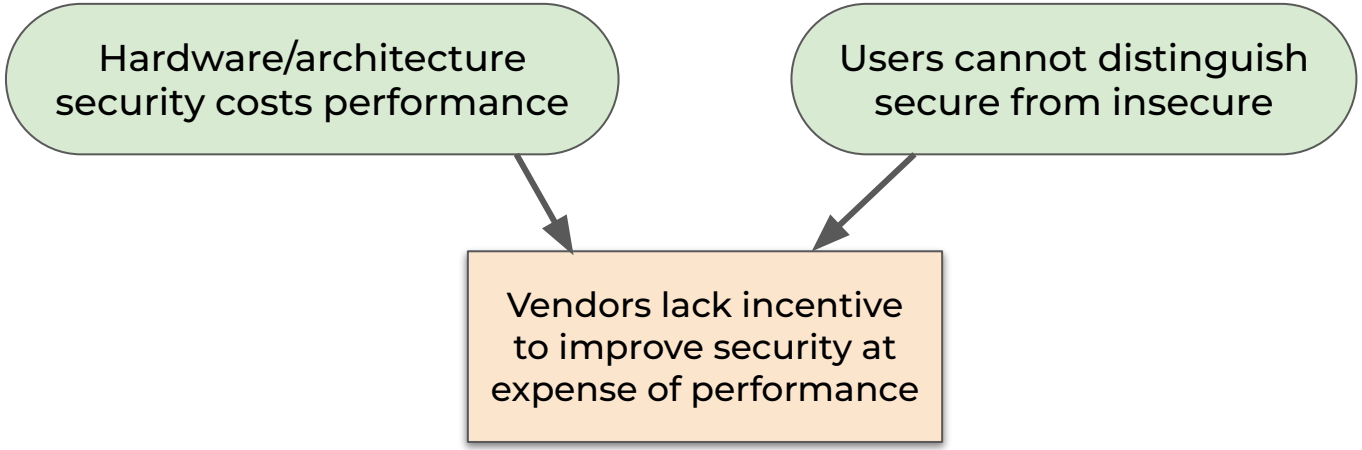


Background

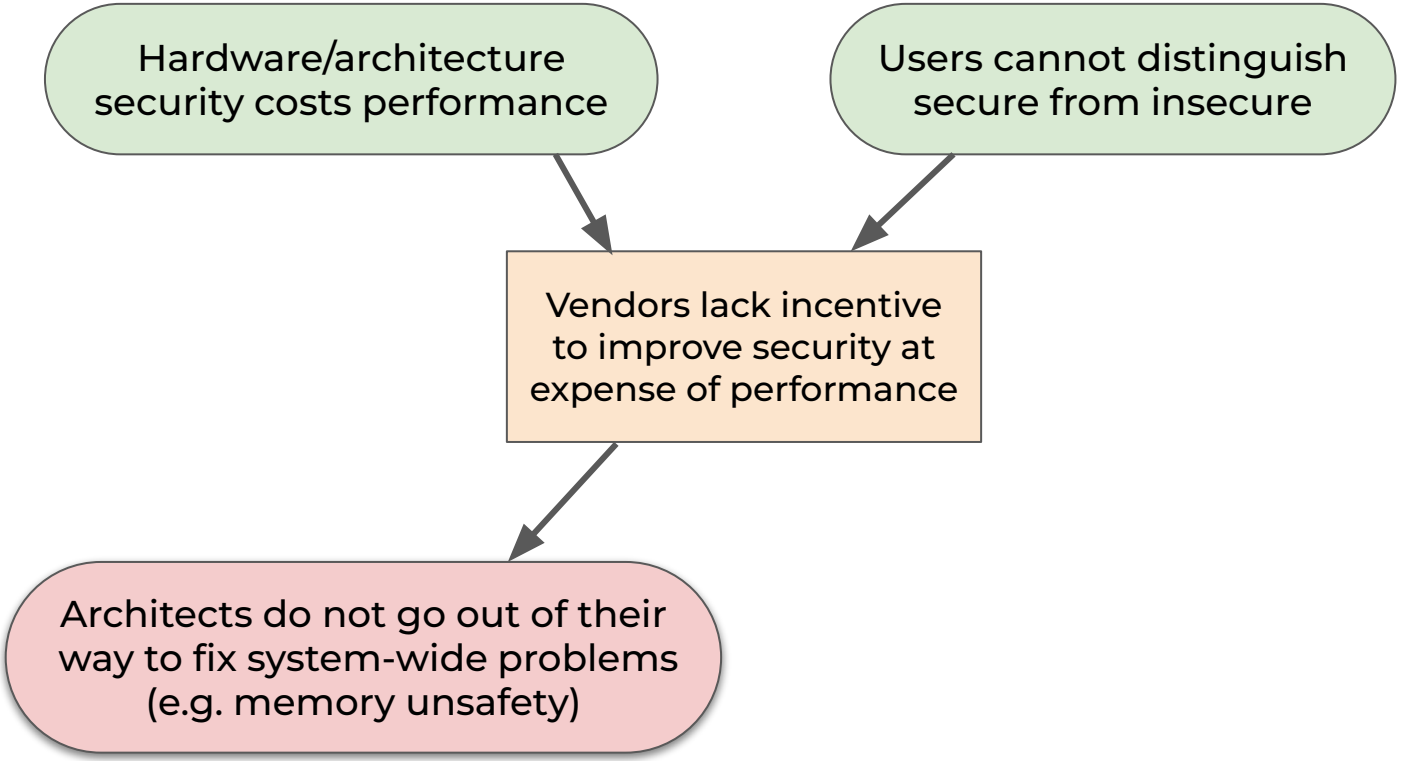
Hardware/architecture security costs performance

Users cannot distinguish secure from insecure

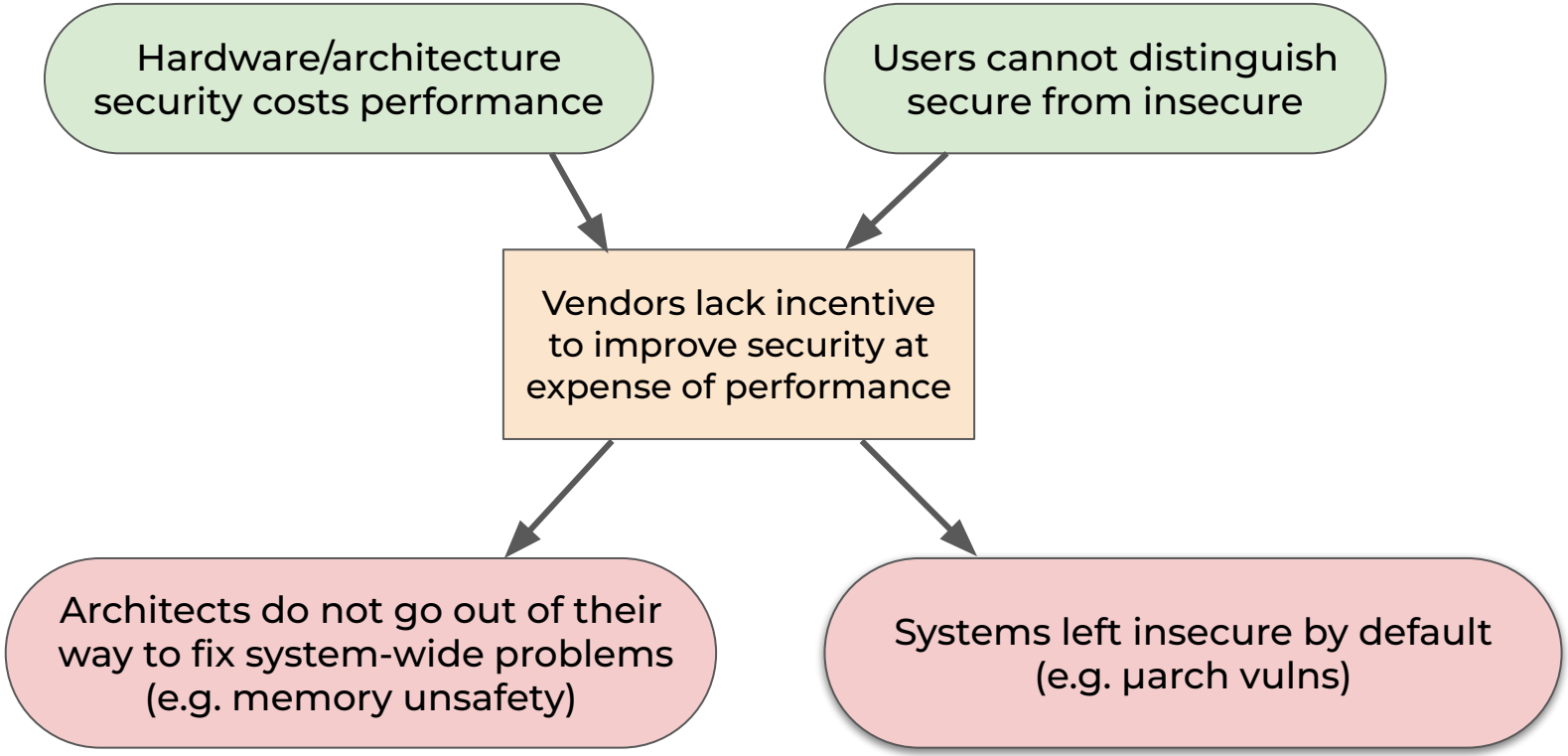
Background



Background



Background



How might architecture be regulated?

- Mandatory cybersecurity labels?
- Mandatory NIST Cybersecurity Framework?
- Vendor liability?
- Addressing weaknesses?
- Prescribing defenses?

How might architecture be regulated?

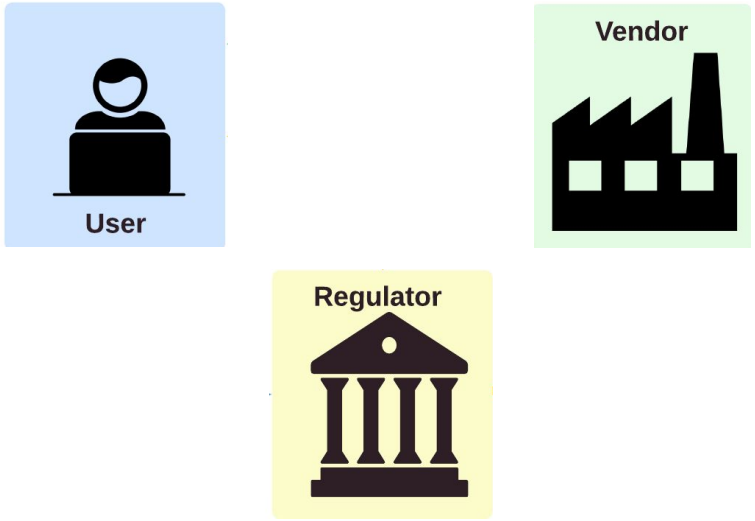
- ~~Mandatory cybersecurity labels?~~
- ~~Mandatory NIST Cybersecurity Framework?~~
- ~~Vendor liability?~~
- ~~Addressing weaknesses?~~
- ~~Prescribing defenses?~~

Existing regulatory approaches will not work if applied to computer architecture

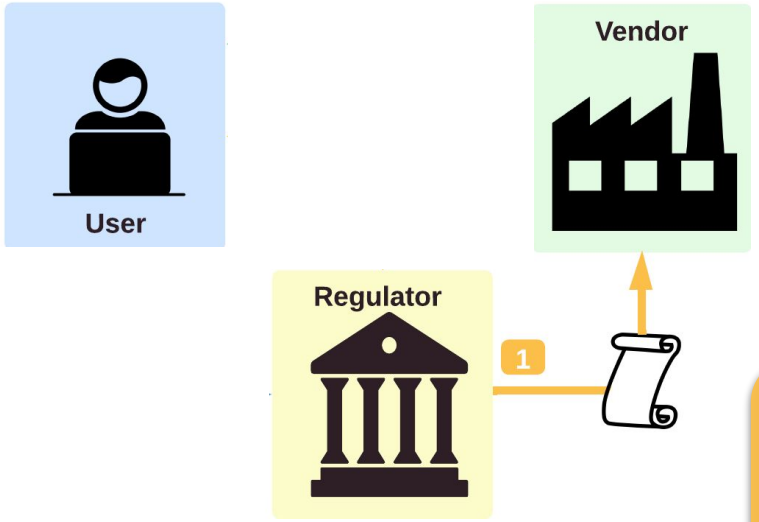
A Proposed Regulation for Computer Architecture Security

Vendors should allocate some fixed percentage of resources on security, **including the resources of systems themselves** (like CPU cycles or energy)

System overview

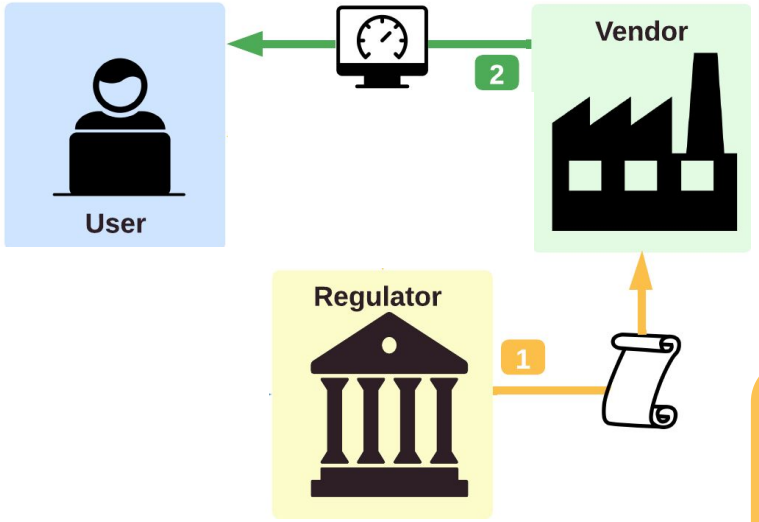


System overview



Regulator issues “flat rate” regulation: Vendors must spend a fixed percentage of resources on security

System overview

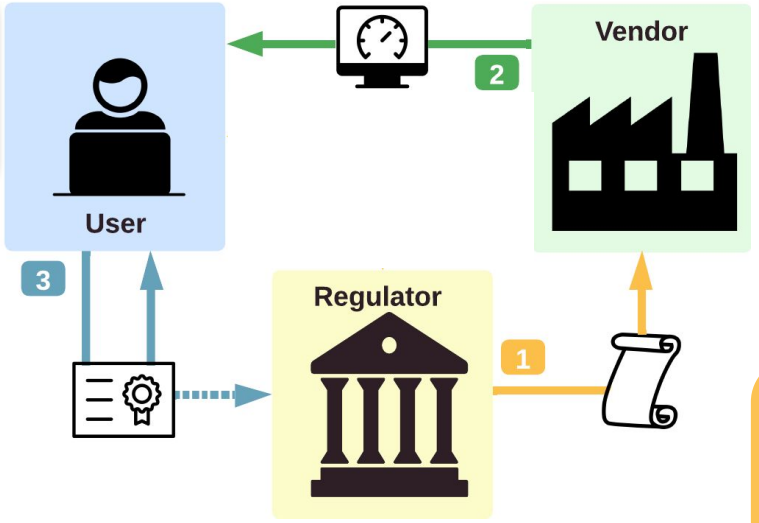


Vendor spends security budget as they see fit. Budget spending is public information. Vendors give products ability to measure on-device security spending

Regulator issues “flat rate” regulation: Vendors must spend a fixed percentage of resources on security

System overview

User verifies product spends sufficient resources on security during runtime. User can report to regulator



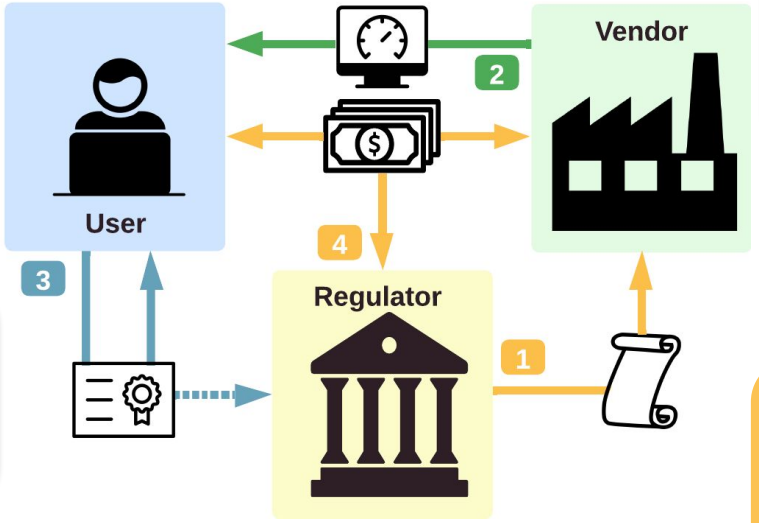
Vendor spends security budget as they see fit. Budget spending is public information. Vendors give products ability to measure on-device security spending

Regulator issues “flat rate” regulation: Vendors must spend a fixed percentage of resources on security

System overview

User verifies product spends sufficient resources on security during runtime. User can report to regulator

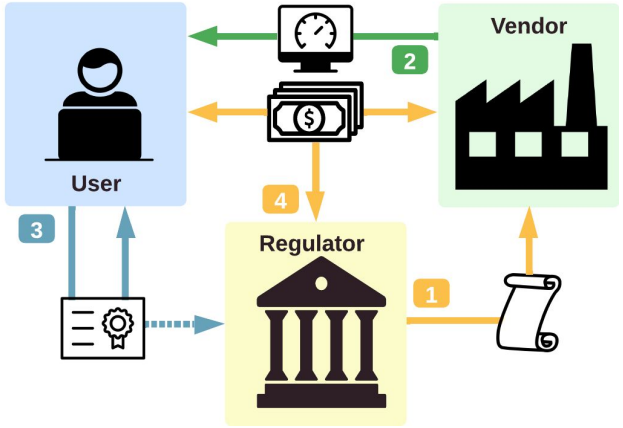
Regulator oversees and mediates the system by adjusting incentives



Vendor spends security budget as they see fit. Budget spending is public information. Vendors give products ability to measure on-device security spending

Regulator issues “flat rate” regulation: Vendors must spend a fixed percentage of resources on security

What does this achieve?



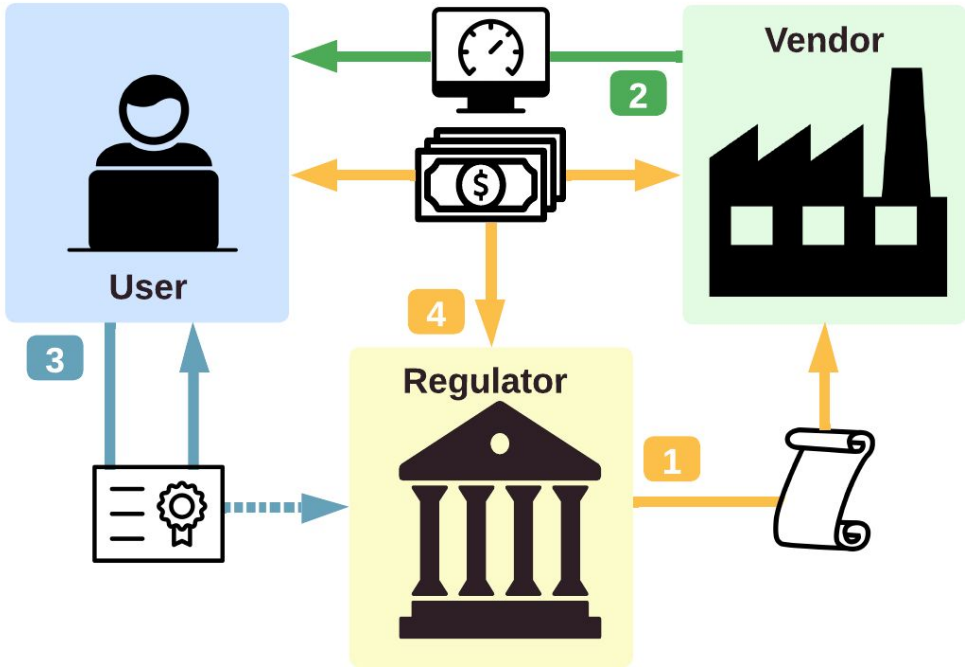
1. All vendors have to spend same amount on security
   a. removes incentive to favor performance over security
   b. sunk cost → no reason to not maximize utility
2. Leaves security decision-making in the hands of the experts
3. Disclosed security allocation → appropriate level of vendor liability

What should the “flat rate” percentage be?

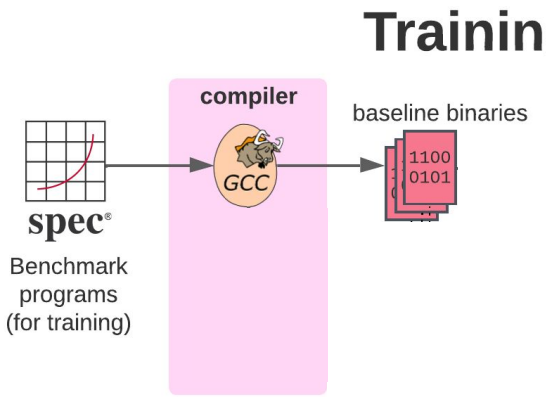
- Simulation/modeling work in the paper addresses this
  - Main finding: More is **not** always better!

- May need to be adjusted depending on type of product or risk level

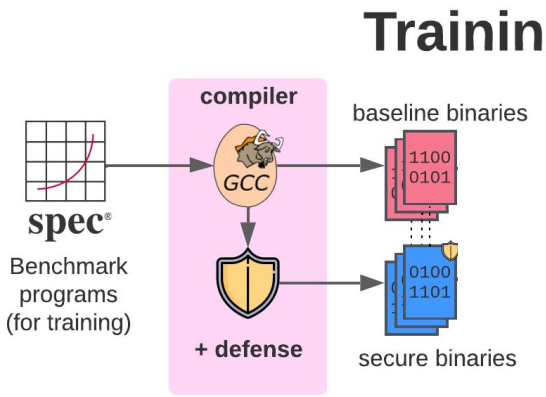
Implementing this is achievable!



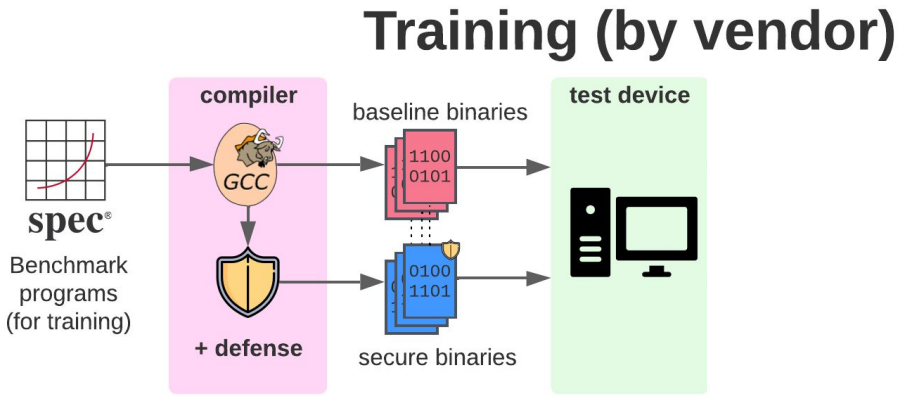
Measuring on-device security overheads



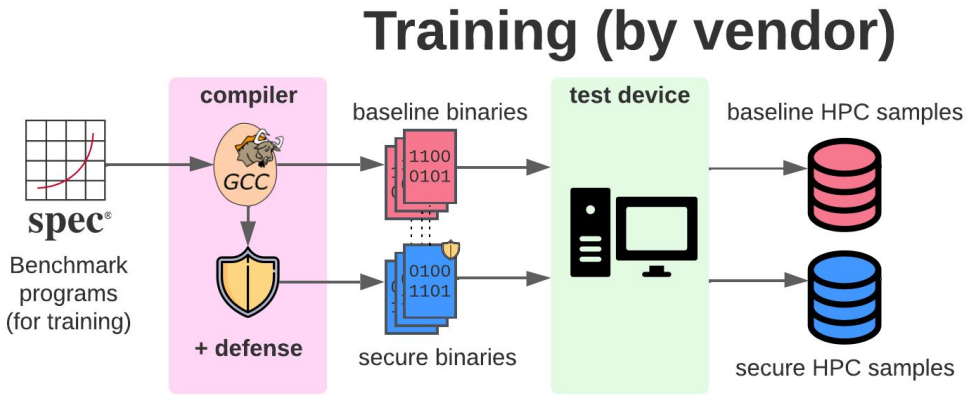
Measuring on-device security overheads



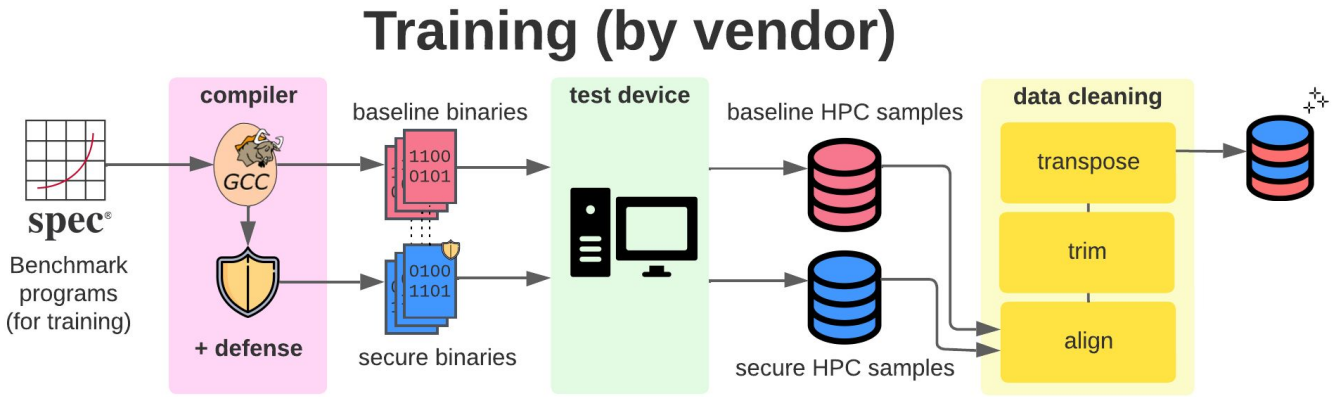
Measuring on-device security overheads



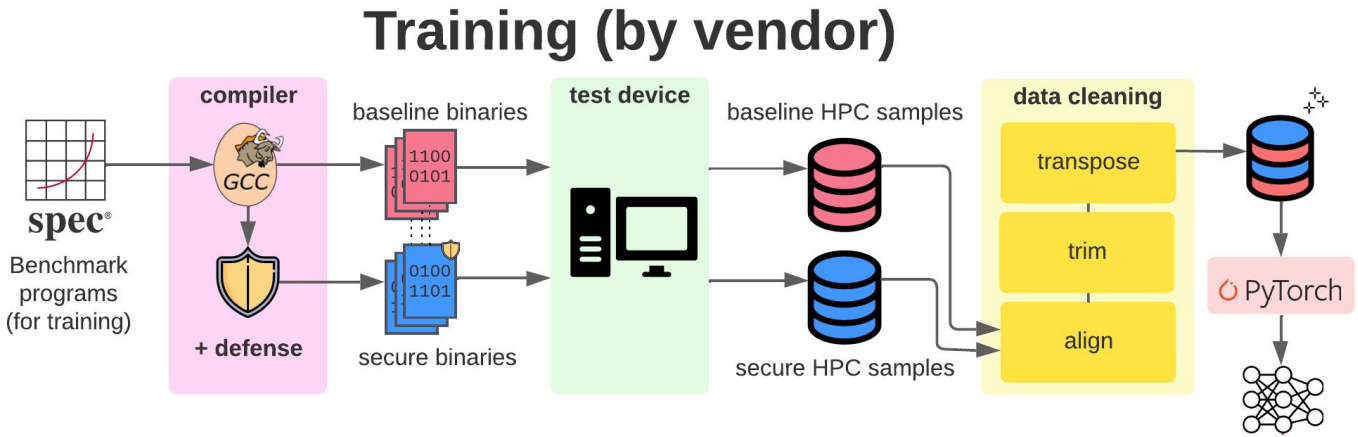
Measuring on-device security overheads



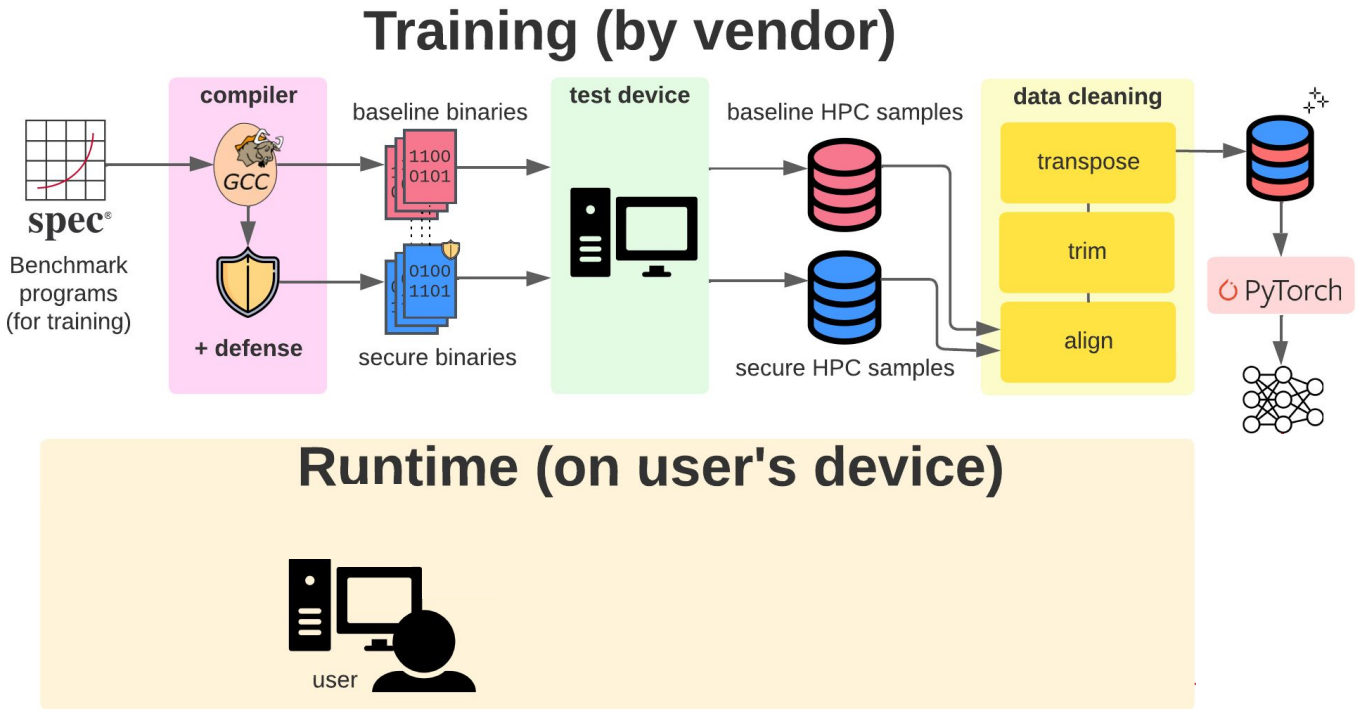
Measuring on-device security overheads



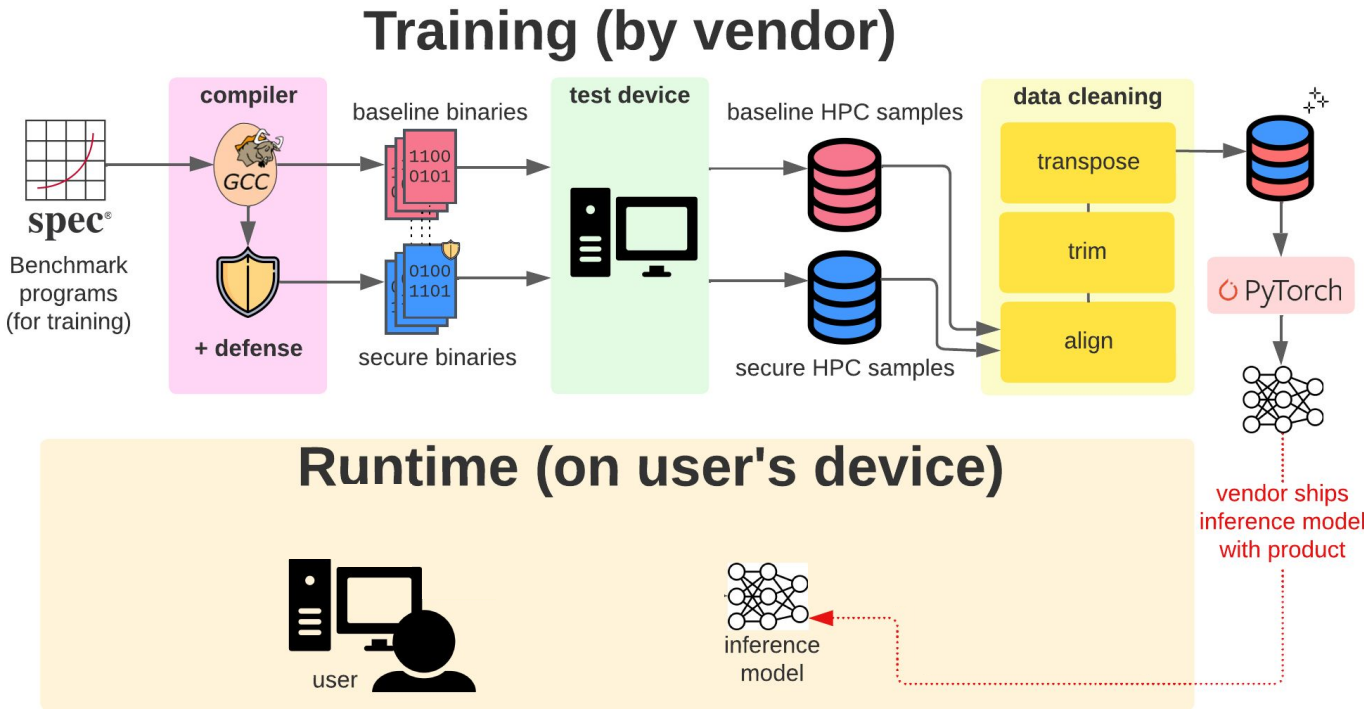
Measuring on-device security overheads



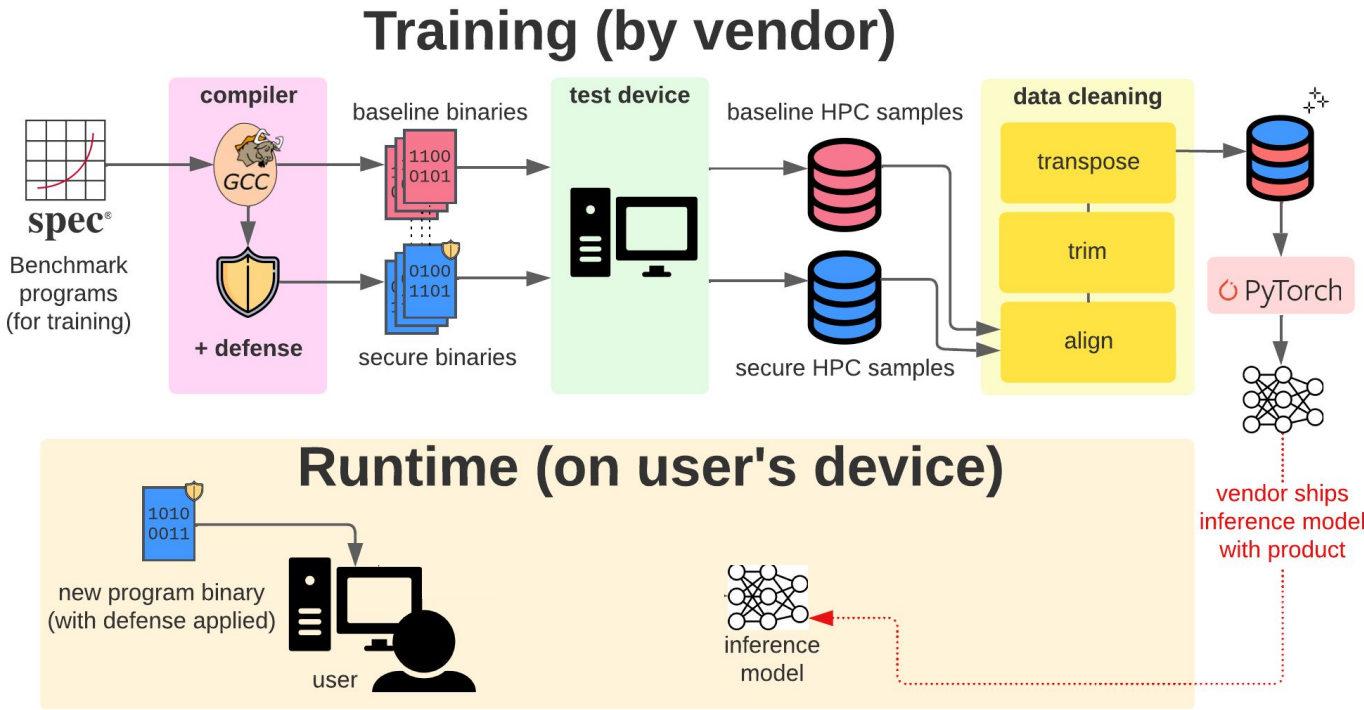
Measuring on-device security overheads



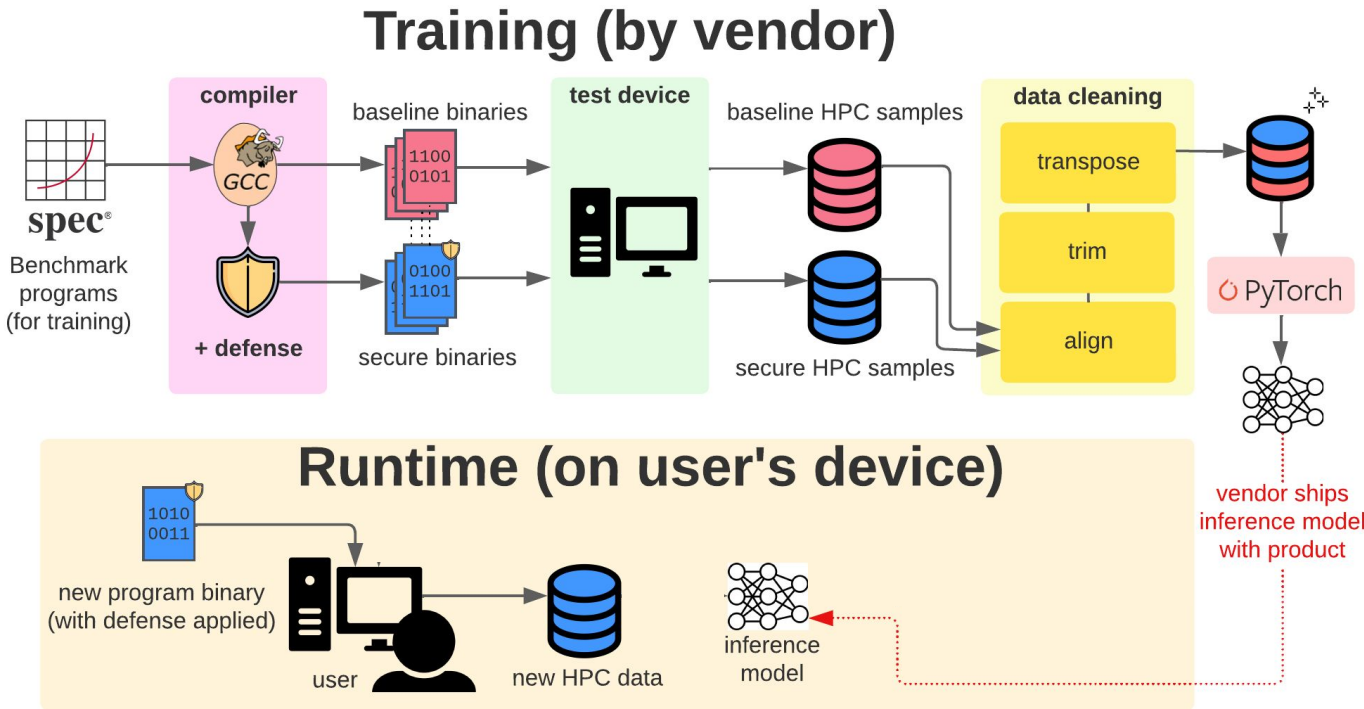
Measuring on-device security overheads



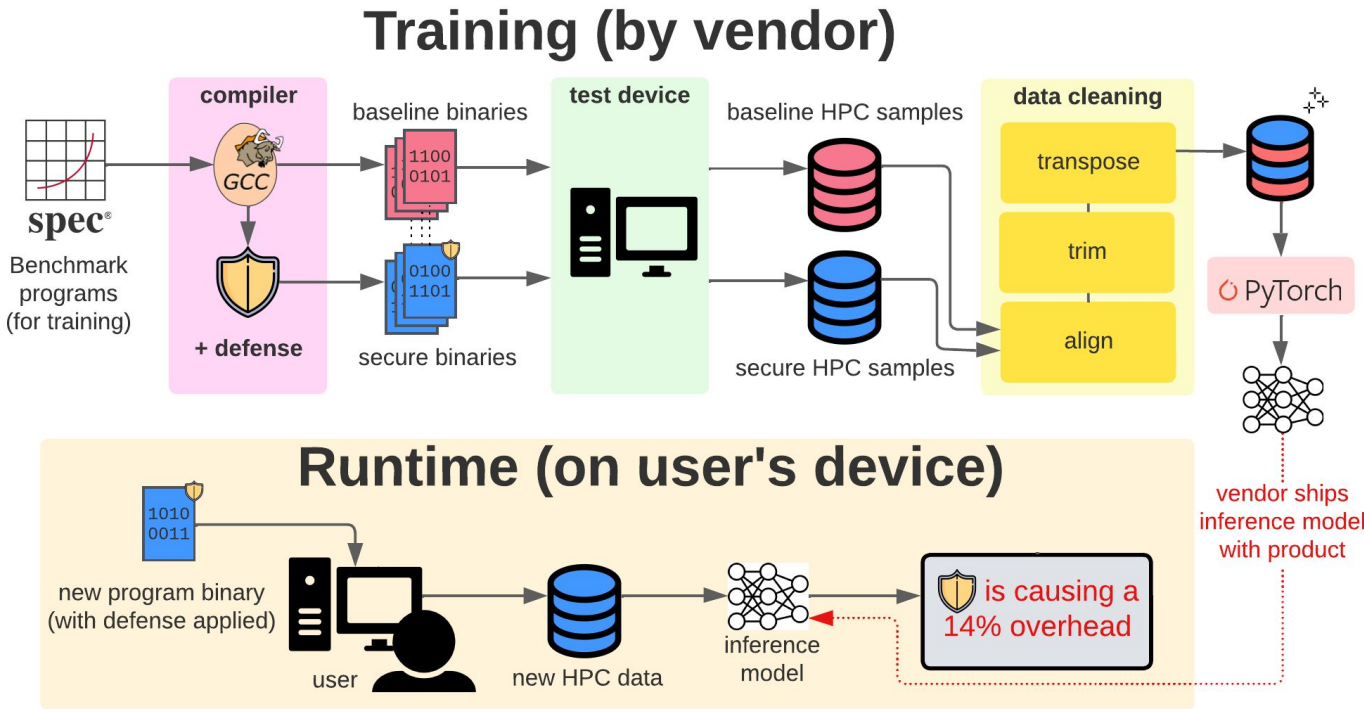
Measuring on-device security overheads



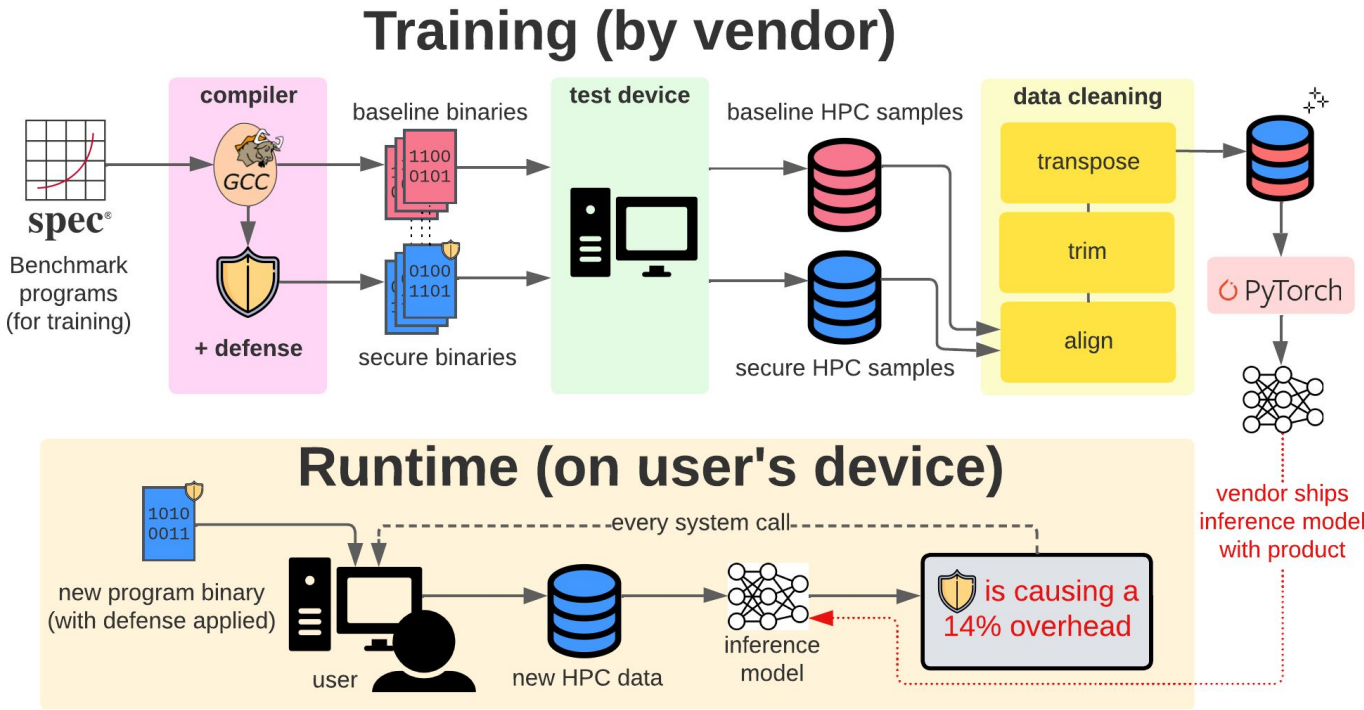
Measuring on-device security overheads



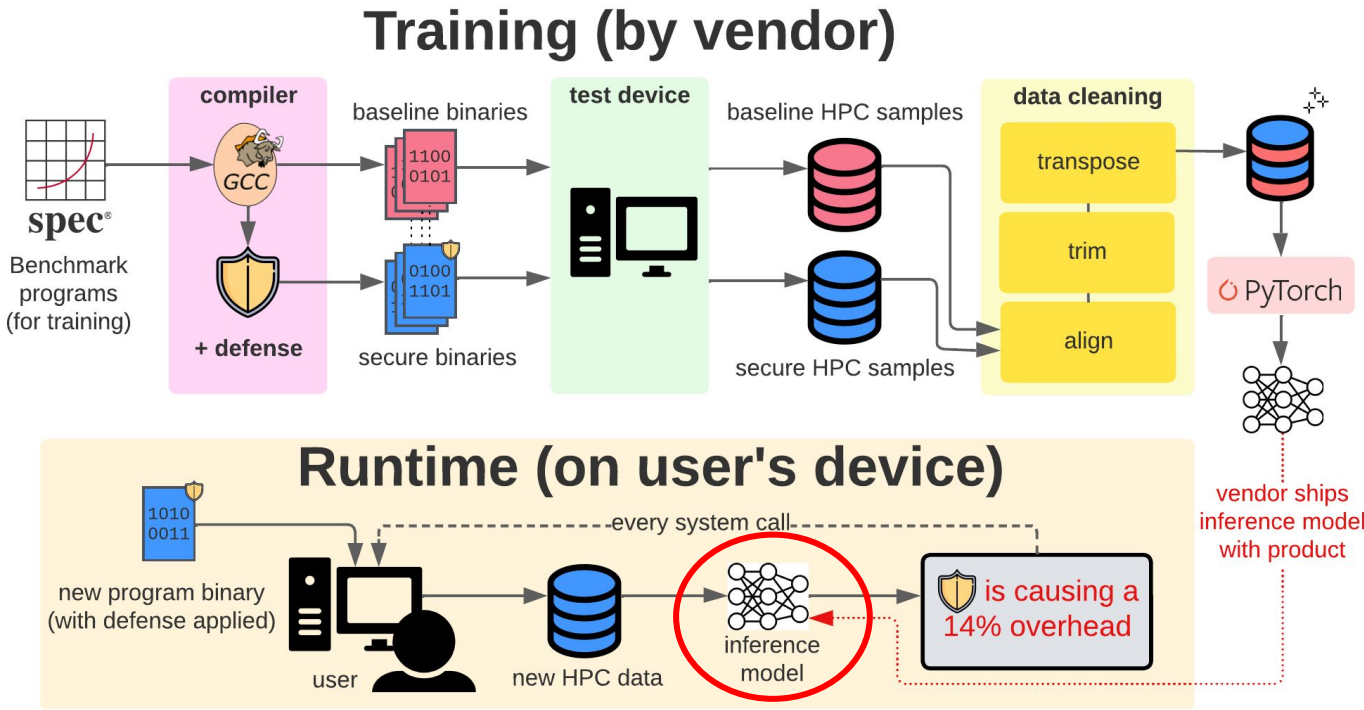
Measuring on-device security overheads



Measuring on-device security overheads

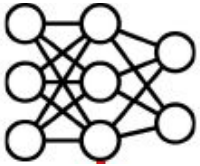


Measuring on-device security overheads



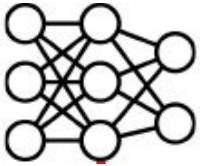
How accurate are the model predictions?

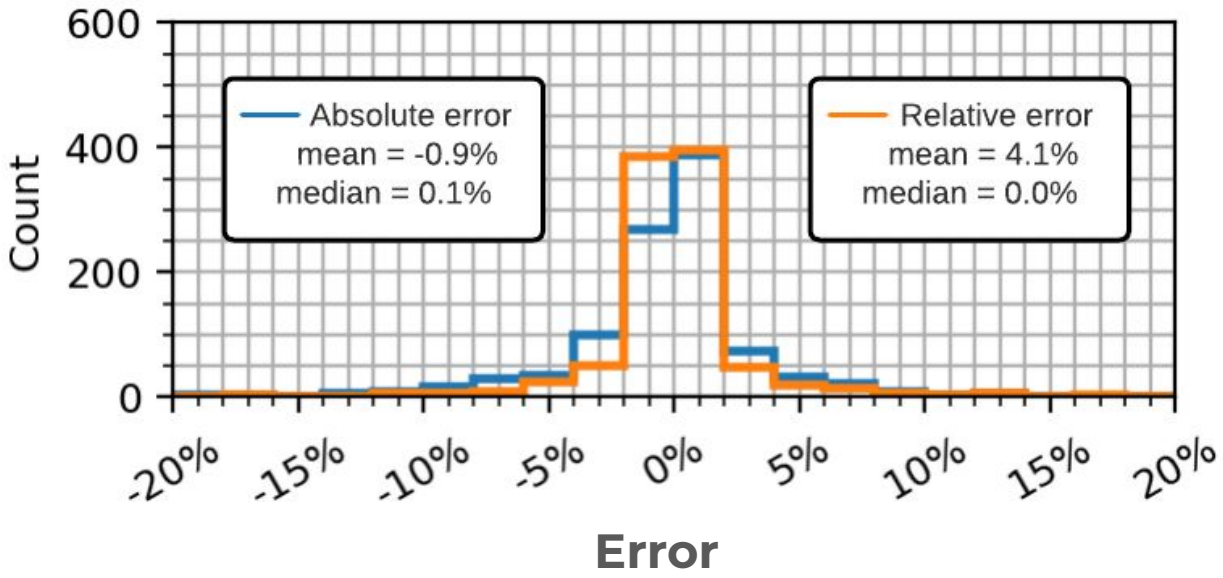
Binary hardening compiler flags



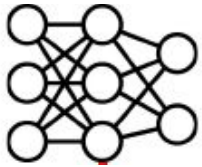
How accurate are the model predictions?

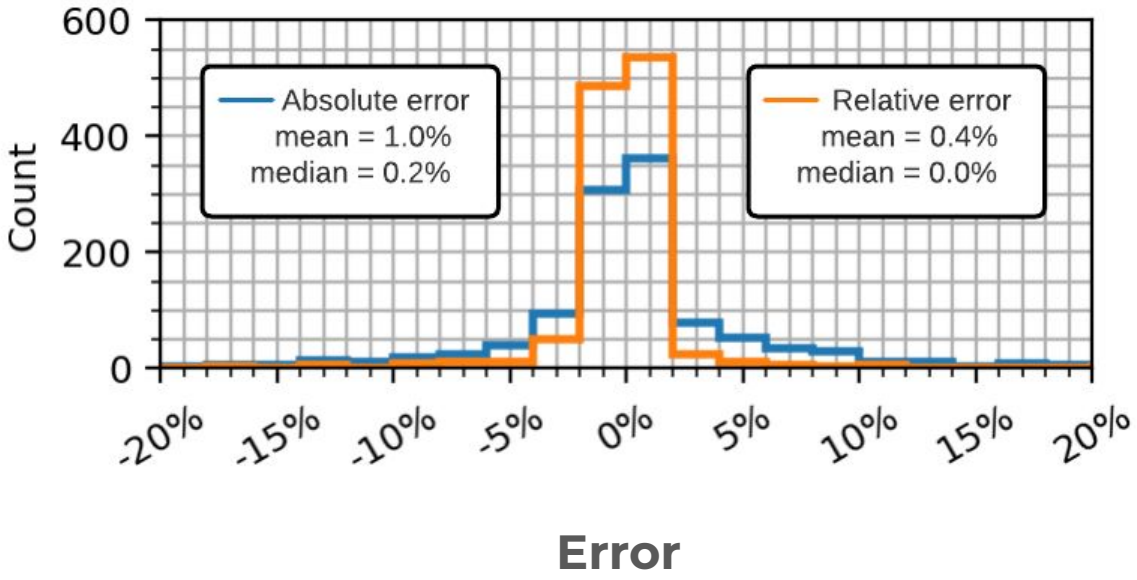
Binary hardening compiler flags



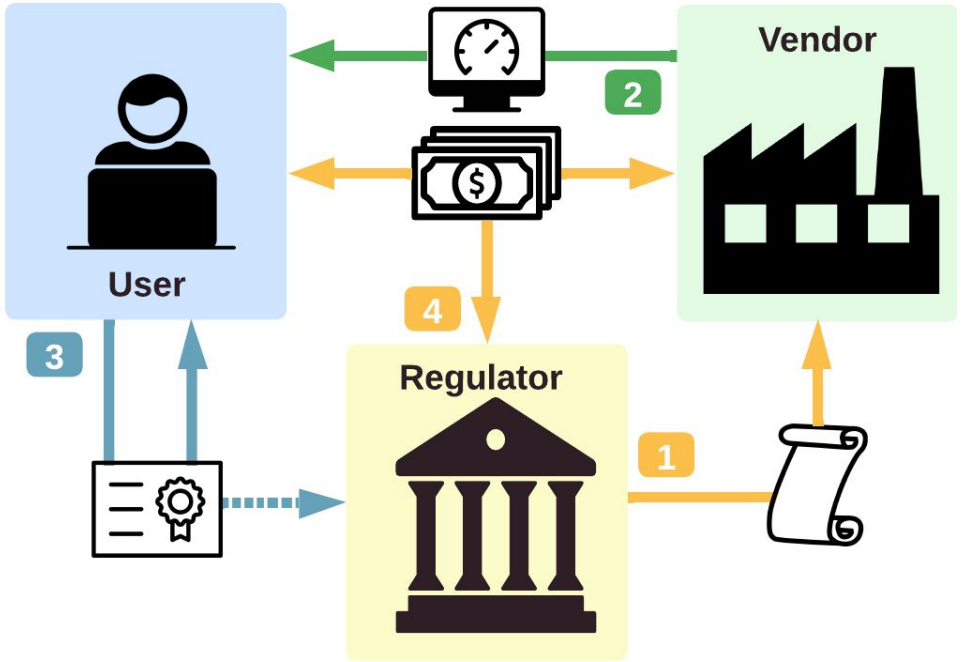


How accurate are the model predictions?





Summary: Flat-rate security tax is practical policy



Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '24, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyberinsurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan

modeling

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

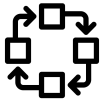
How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '24, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

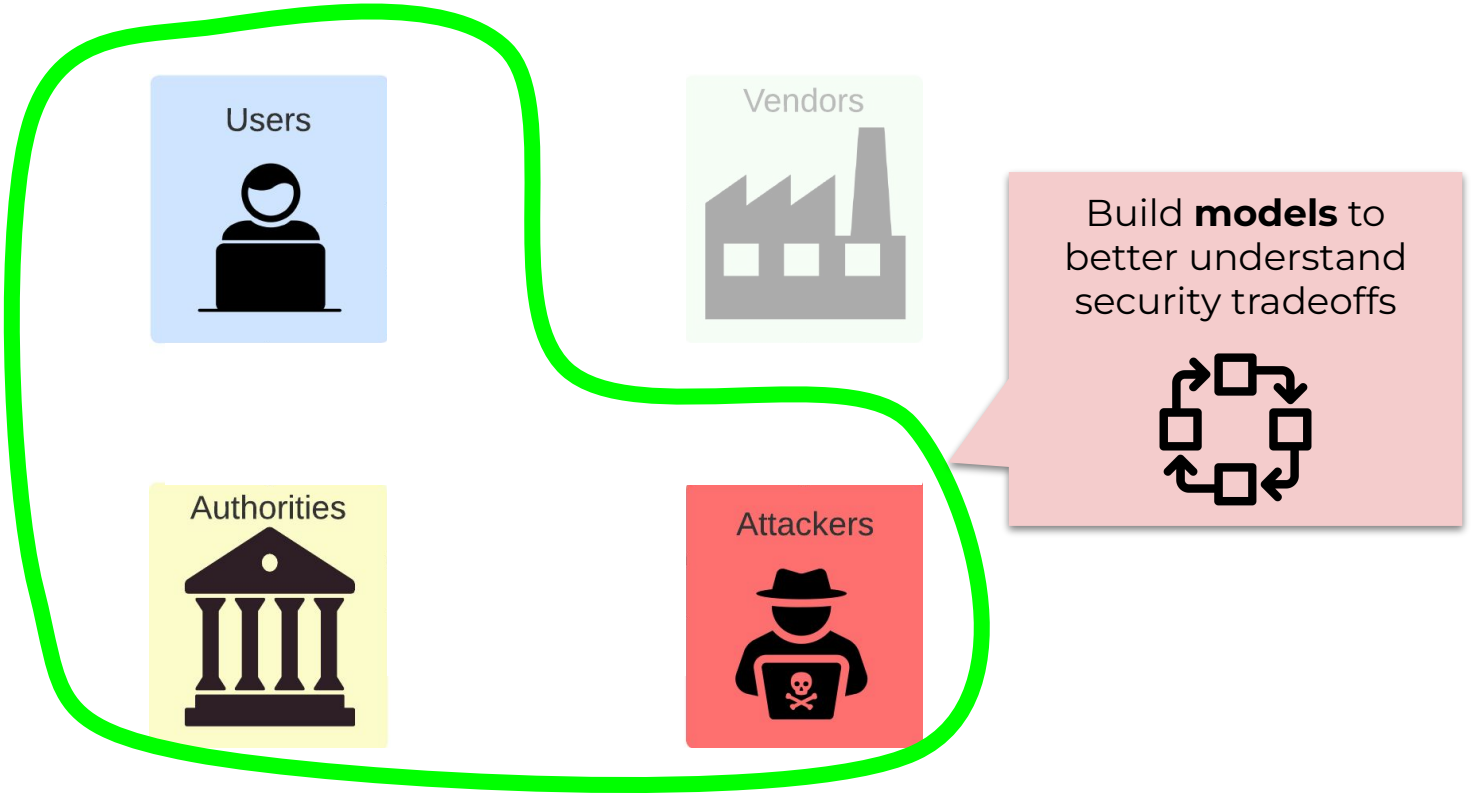
mechanisms

Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan



modeling

Simulations of Cyber Insurance Tradeoffs



Background

- Cyber insurance = insurance to cover risk of cyber attack
- Cyber insurance is a proposed mechanism for improving security
- Theory:
  - Insurers want to collect premiums and don't want to pay claims
  - → Insurers have incentive to accurately quantify risks and price policies accordingly
  - → Insurers will learn which security tradeoffs are worth making
  - → Insurers will offer lower premiums to less risky customers
  - → Cyber insurance will produce a virtuous cycle of security improvements

Real-world state of cyber insurance

- Surprising **lack of sophistication** in pricing policies — *Romanosky et al., 2019*
- Insurers **only offer a marginal incentive to invest in security** — *Woods & Moore, 2019*
- **Rising premiums, lowered coverage** — *GAO, 2021*
- **3 out of 4 top insurers had unprofitable loss ratios** in recent years — *Woods 2023*
- Lawyers typically suggest **obfuscating root causes**— *Woods et al., 2023*

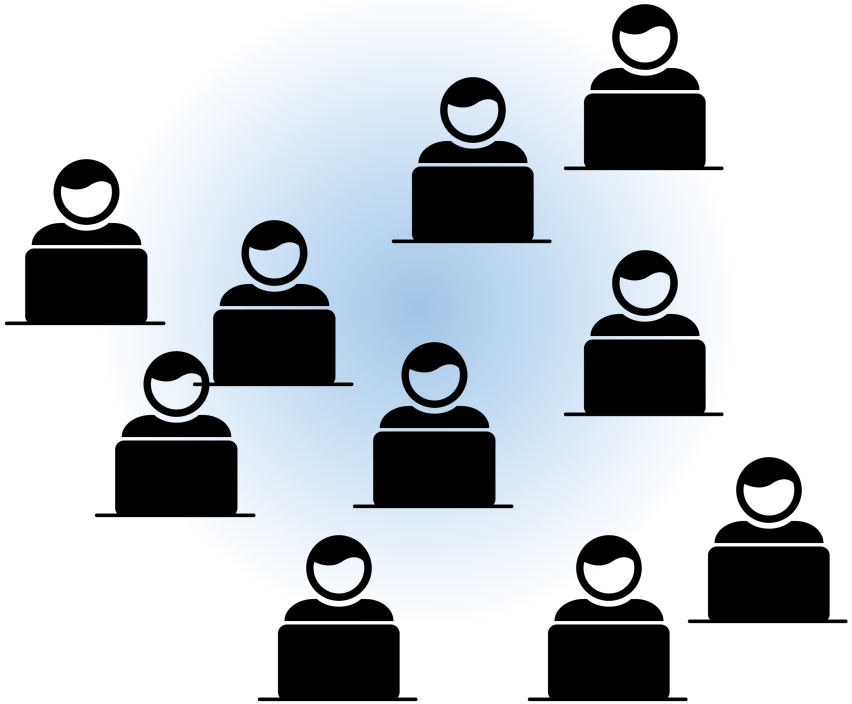
Understanding effect of insurance via modeling

- Prior works use one-shot game mathematical modeling
- Very few works use multi-shot iterated games
  - Outcomes cannot be determined analytically—must be simulated!
- My work: Monte Carlo simulations of an adversarial security game between attackers and defenders

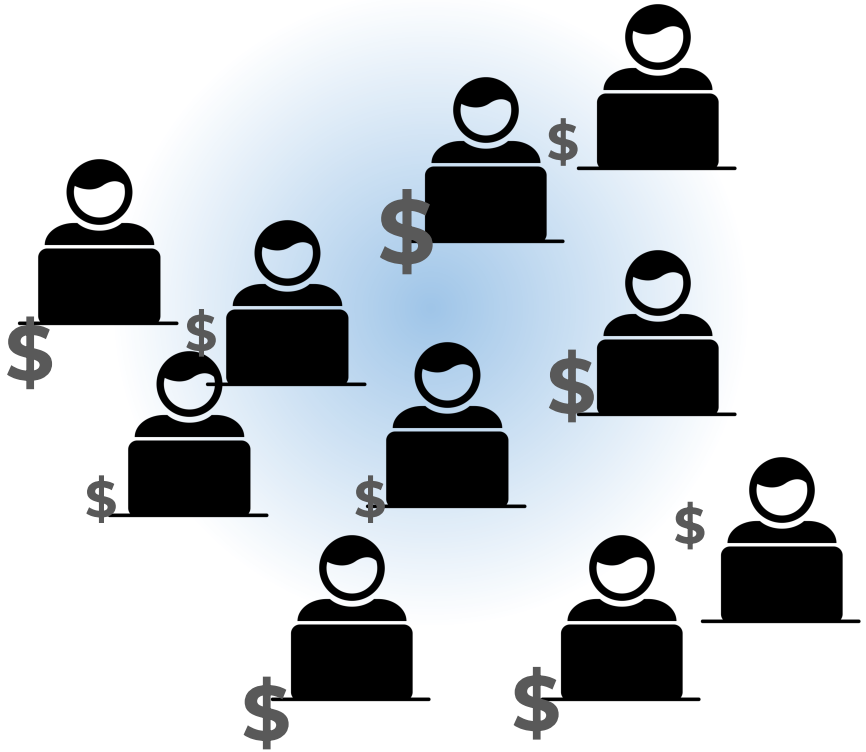
Heuristics

- Attackers and Defenders initialized with assets drawn from lognormal distribution
- Defenders are imbued with a “security posture” parameter
- Defenders can make rational decisions between improving security or buying insurance
- Insurers base policy premiums on expected losses

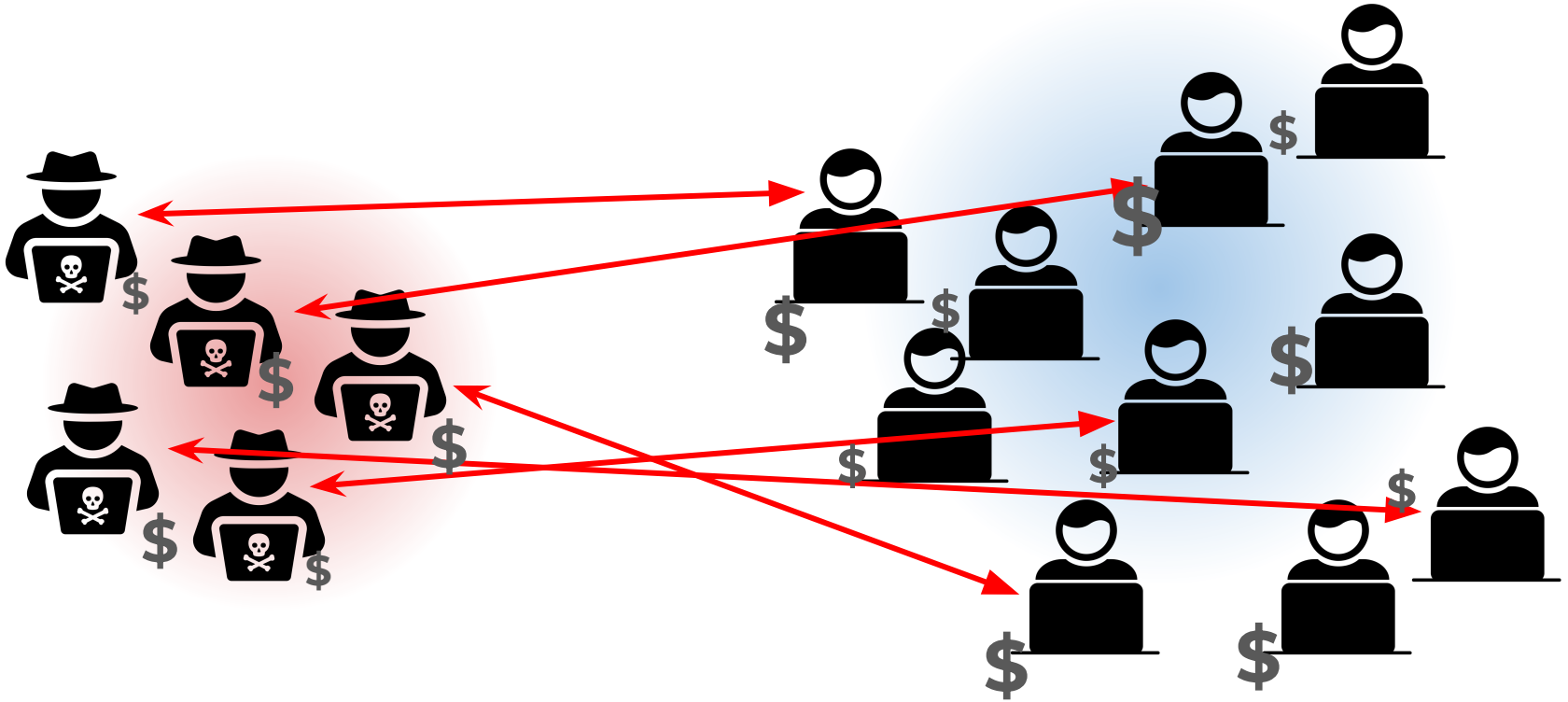
Gameplay



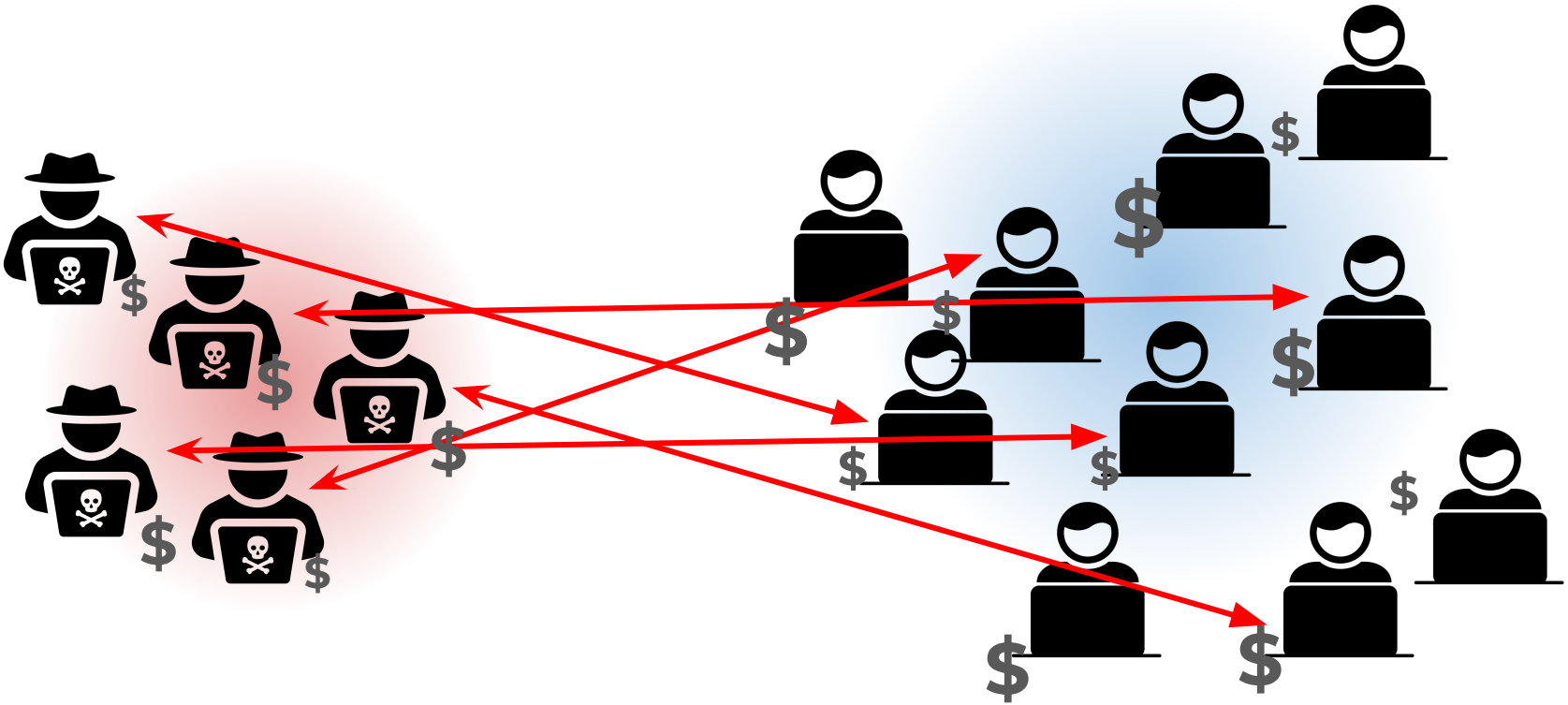
Gameplay



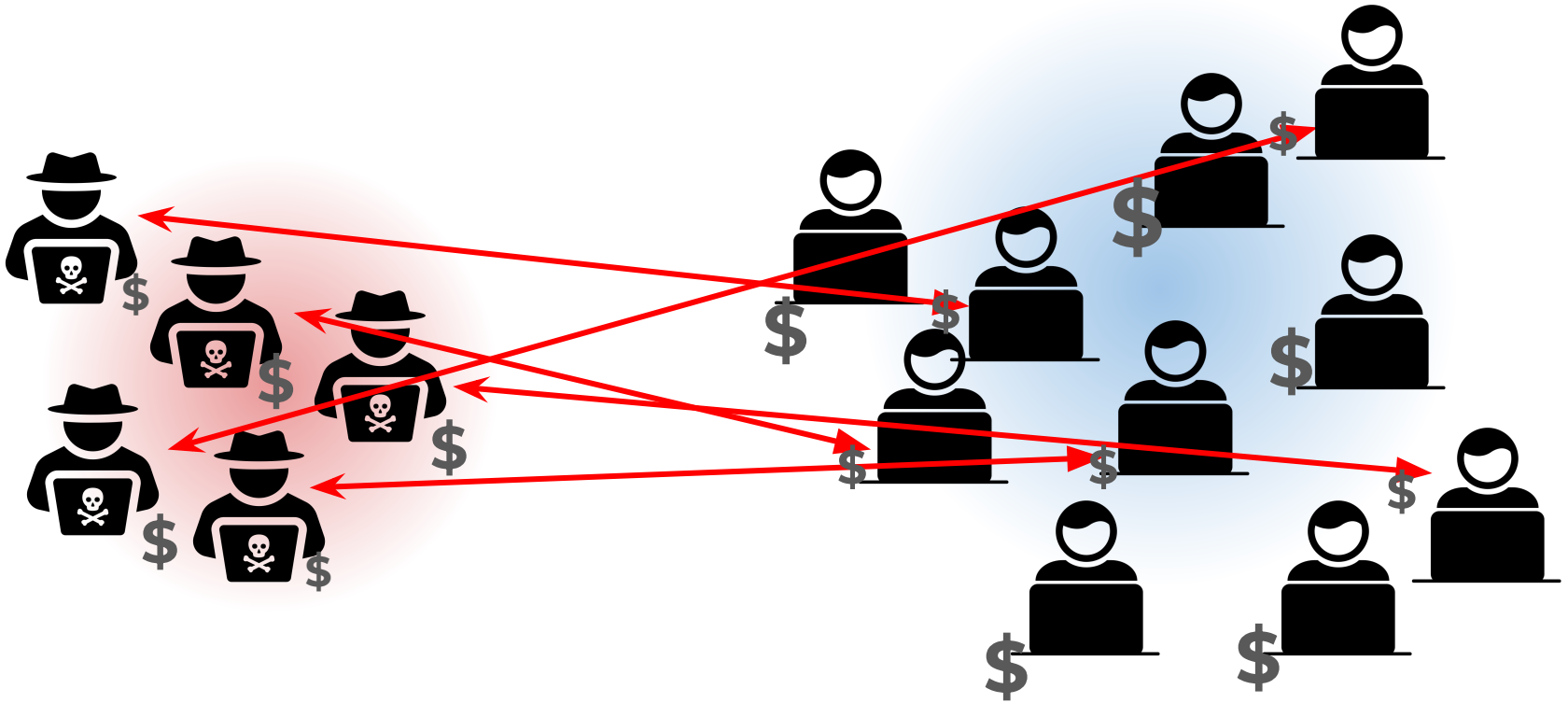
Gameplay



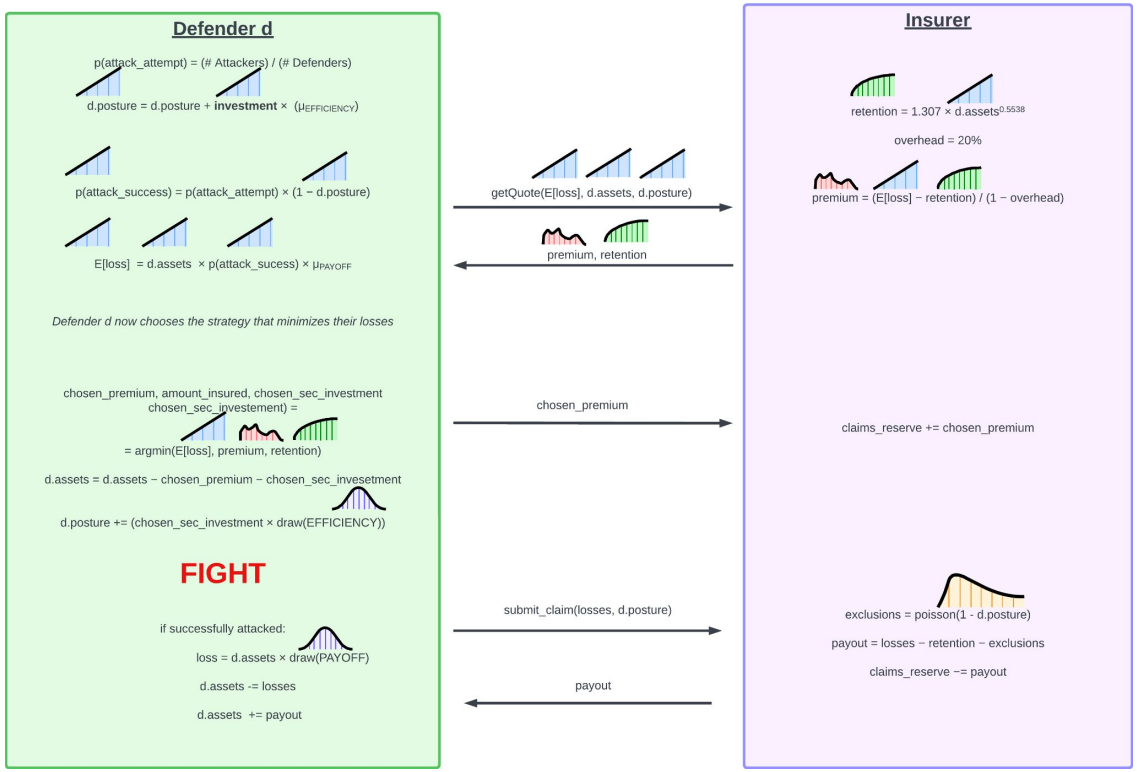
Gameplay



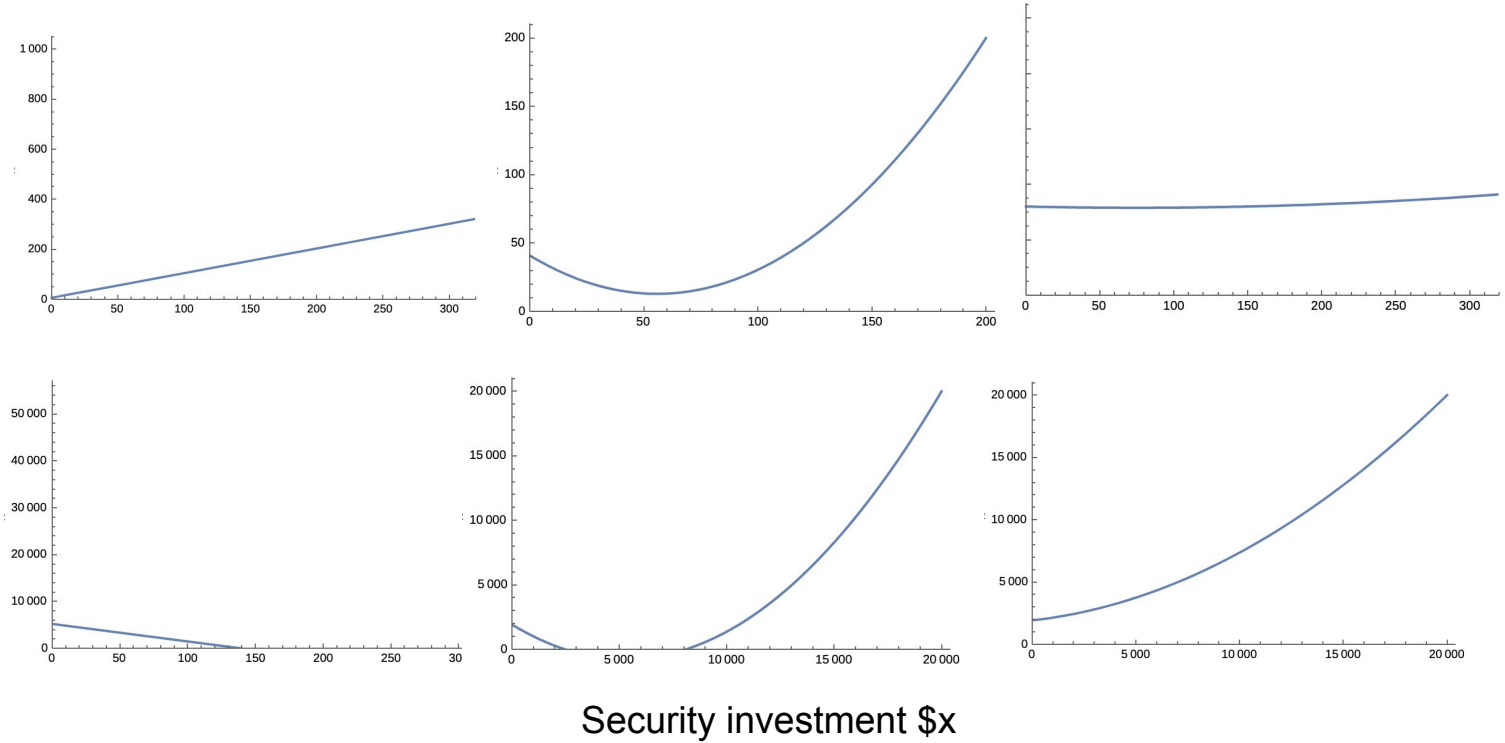
Gameplay



Defender makes rational choice between security, insurance



Optimal strategy depends on conditions



Next Steps

- Model is built
- Just need to run and collect data
- Hypotheses:
  - Does insurance improve security outcomes? If so, how?
  - Does the existence of multiple insurers create a “race to the bottom”?
  - Is there an optimal amount of insurance? Is it non-zero!

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

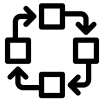
How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '24, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan



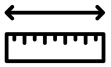
modeling

Talk Outline

A New Doctrine for Hardware Security (*ASHES 2020*)
Adam Hastings, Simha Sethumadhavan

foundation

How Much is Performance Worth to Users? (*CF'23*)
Adam Hastings, Lydia Chilton, Simha Sethumadhavan

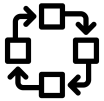


measurements

Incentivizing the Creation and Adoption of Architectural Mechanisms for Security (CAL '24, under submission *ISCA '24*)
Adam Hastings, Ryan Piersma, Simha Sethumadhavan

mechanisms

Simulations of Cyber Insurance Tradeoffs *(in progress)*
Adam Hastings, Simha Sethumadhavan



modeling

Timeline

- Dec. 2023 — Thesis Proposal
- Feb. 2024 — Cyber Insurance submission (Usenix Security)
  - May 2024 — Author notification
- June 2024 — Thesis Defense

The Economics of Hardware Security

Thesis Proposal | 2023 December 11

Adam Hastings