Security Heroes versus the Power of Privacy

PRIVACY
is worth fighting for

Professor Privacy

Protecting rights of individuals!

Minimizing data abuse!

Analyzing and fixing systems!

Protecting your privacy

Captain Security

Protecting systems!

Limiting user privileges!

Finding weaknesses
and exploiting them!

MISCONCEPTIONS!

I have nothing to hide!

SECRET IDENTITIES

Nothing to hide??

"Tesla workers shared images from car cameras, including "scenes of intimacy"

Ars Technica, April 2023

"Roomba testers feel misled after intimate images ended up on Facebook"

MIT technology review, Jan 2023

We don't have user secrets!

Personal data

entails more than you think

Not ‘just’ personal data

Inferring pregnancy

We don’t need privacy!

We have security!

Privacy is NOT confidentiality

Unlinkability

Disassociability

Transparency

Predictability

Intervenability

Manageability

M. Hansen, M. Jensen and M. Rost, "Protection Goals for Privacy Engineering," 2015
NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems, 2017

Deducing new information from personal data

WANT TO KNOW MORE?

We hope you will not read this part because when you click on this link you will sell us your soul.

YES!
SHOW ME THE COOL STUFF

No. I am a boring person

CLASH OF THE THE TITANS

SECURITY

Care about your system

PRIVACY

Care about others

(which will help to take care of yourself)

Companies don’t want privacy!

It costs too much!

Benefits equal x2 privacy investment

WHAT HAPPENS WHEN THINGS GO WRONG??

Insurance

For when the house burns down

Incidents

Due diligence protects against regulatory fines

Security Breach

Minimizing data reduces blast radius of breach

We can’t do privacy!

because it breaks everything!

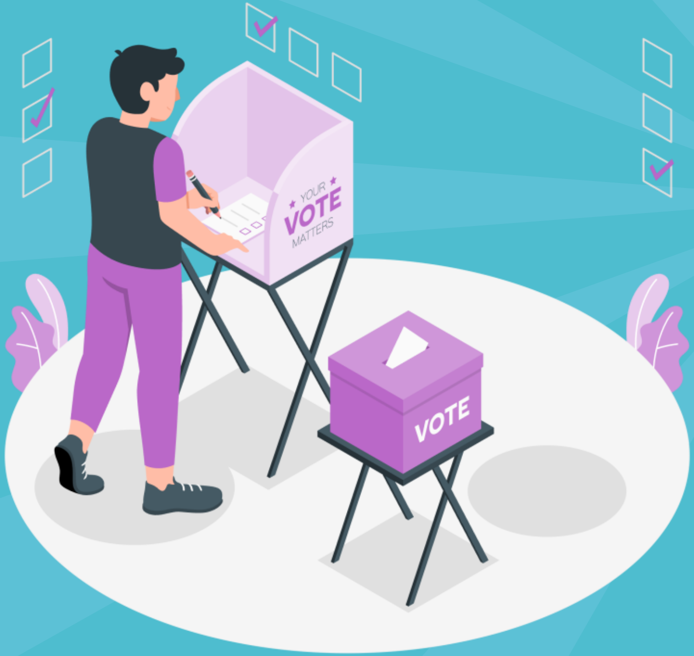
Only True Heroes Allowed!

Authentication vs. anonymity

How do we restrict entry only for members, without knowing who you really are?

Anonymous Communications

How do we contact the Hero when we need them??



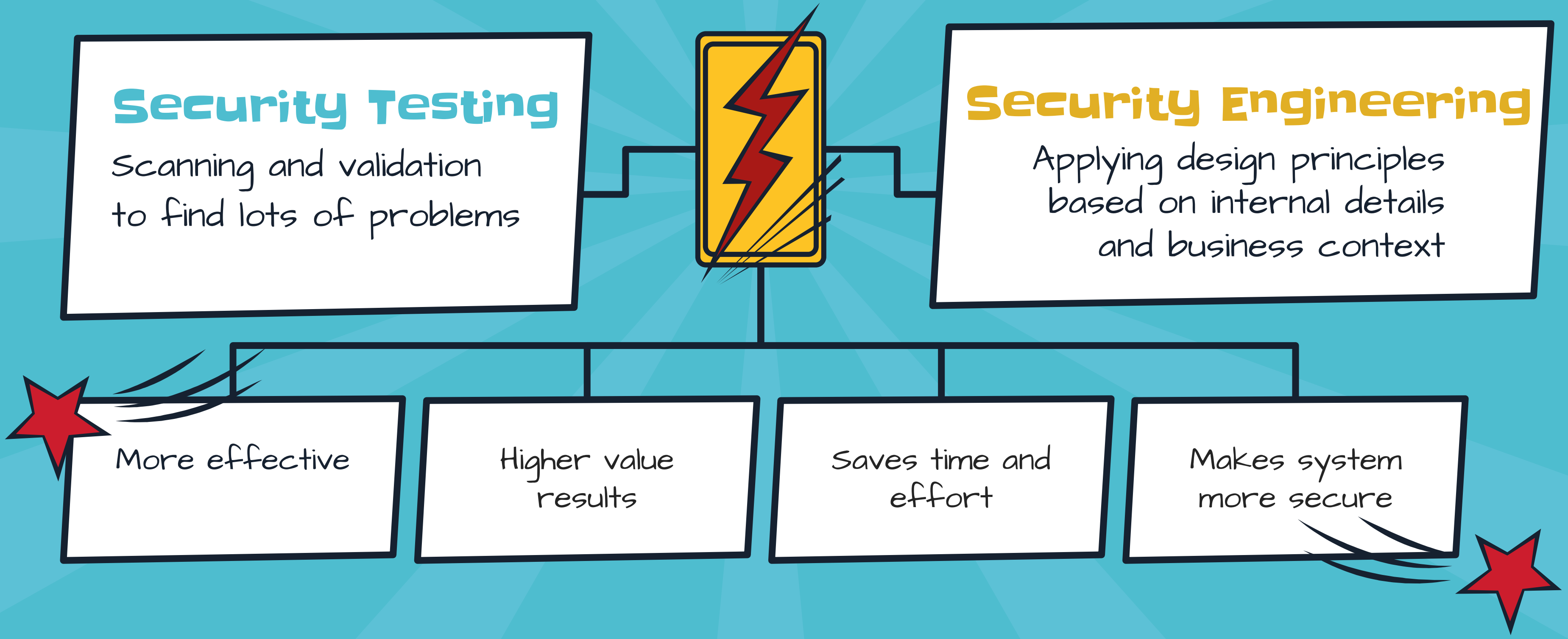
Proof you voted

Without revealing how you voted

Embed privacy by design

Security is about breaking stuff, magik crypto dust and exploiting vulns

Security By Design



Security Testing

Scanning and validation to find lots of problems

Security Engineering

Applying design principles based on internal details and business context

More effective

Higher value results

Saves time and effort

Makes system more secure

Threat Modeling!

Analyzing **representations** of a system to highlight **concerns** about **security** and **privacy** characteristics

Threat Modeling Manifesto

ThreatModelingManifesto.org

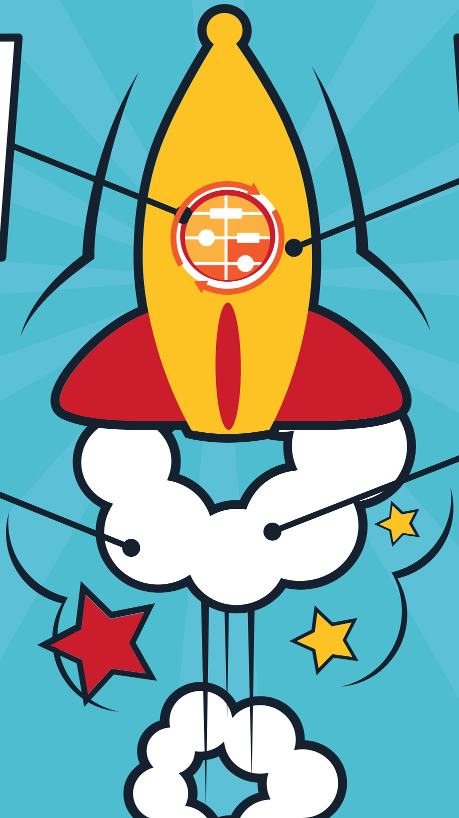
Ask these four questions!

01 What are we working on?

02 What can go wrong?

03 What will we do about it?

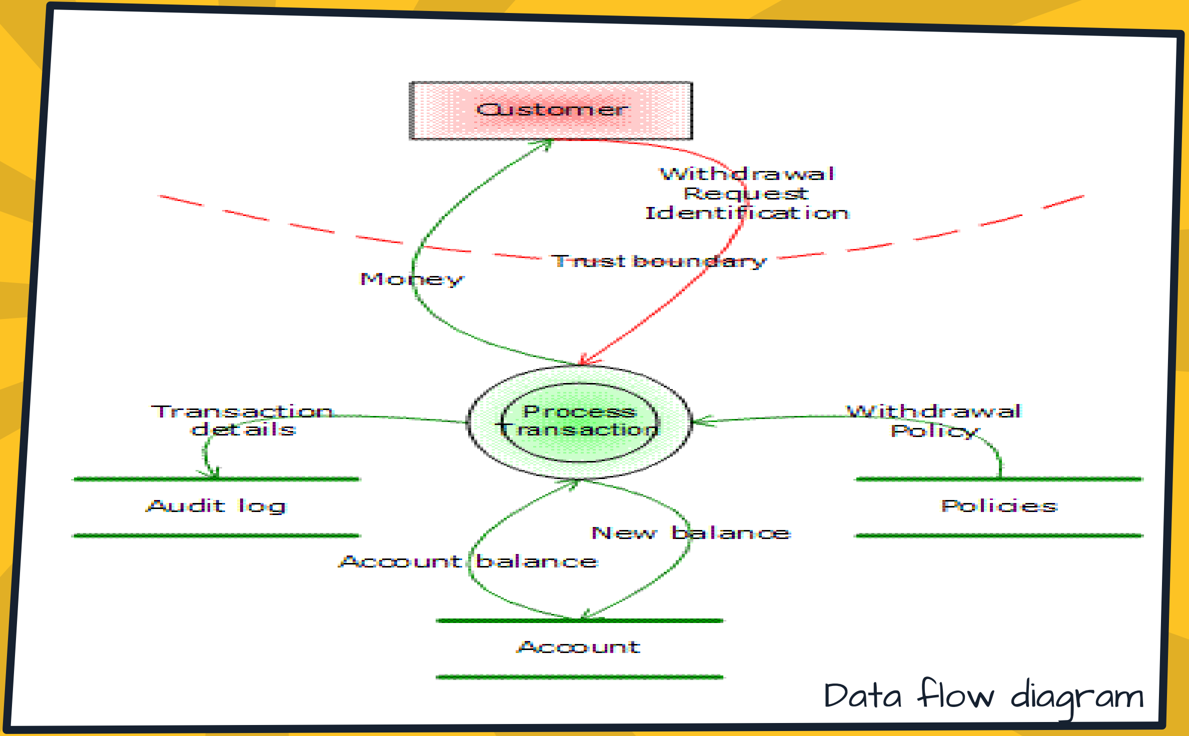
04 Did we do a good job?



Secret Map of the Hidden Layer

All models are wrong

Threat model every flow



Data flow diagram

Revealing Nefarious Threats!

S

Spoofing

Attack on IDENTITY!

T

Tampering

Attack on INTEGRITY!

R

Repudiation

Attack on PROVABILITY!

I

Information Disclosure

Attack on CONFIDENTIALITY!

D

Denial of Service

Attack on AVAILABILITY!

E

Elevation of Privileges

Attack of AUTHORITY!

Unconvering Villainous Schemes!

Privacy threats on the individual

L

Linking

Attack on UNLINKABILITY

I

Identifying

Attack on ANONYMITY

N

Non Repudiation

Attack on PLAUSABLE DENIABILITY

D

Detecting

Attack on UNOBSERVABILITY

D

Data Disclosure

Attack on MINIMALITY

U

Unawareness

Attack on TRANSPARENCY & CONTROL

N

Non Compliance

Attack on BEST PRACTICES

Utility belt

2 Spoofing: An attacker could squat on the random port or socket that the server normally uses.

J Spoofing: An attacker could steal credentials stored on the client and reuse them.

3 Tampering: An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto.

K Tampering: An attacker can load code inside your process via an extension point.

7 Information Disclosure: An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection.

6 Denial of Service

An attacker can make a server unavailable or unusable without ever authenticating, but the problem goes away when the attacker stops **(server, anonymous, temporary)**.

Q Repudiation: An attacker can say "I didn't do that," and you would have no way to prove them wrong.

K Elevation of Privilege: An attacker can inject a command that the system will run at a higher privilege level.

Elevation of Privilege

The requests from a user to the system are linked through identifiers.

1. Is there an identifier (unique within the system or for the session) or dataset?
2. Is there other data associated with that identifier?
3. Is there previous data with the same identifier to which new data can be linked?

- An email address as ID can be used to link all activity to the same user even across multiple services where that email address is used.
- IP address can be used to link multiple visits to the same user.
- All product views in a web shop are linked to the same user because they are logged in.

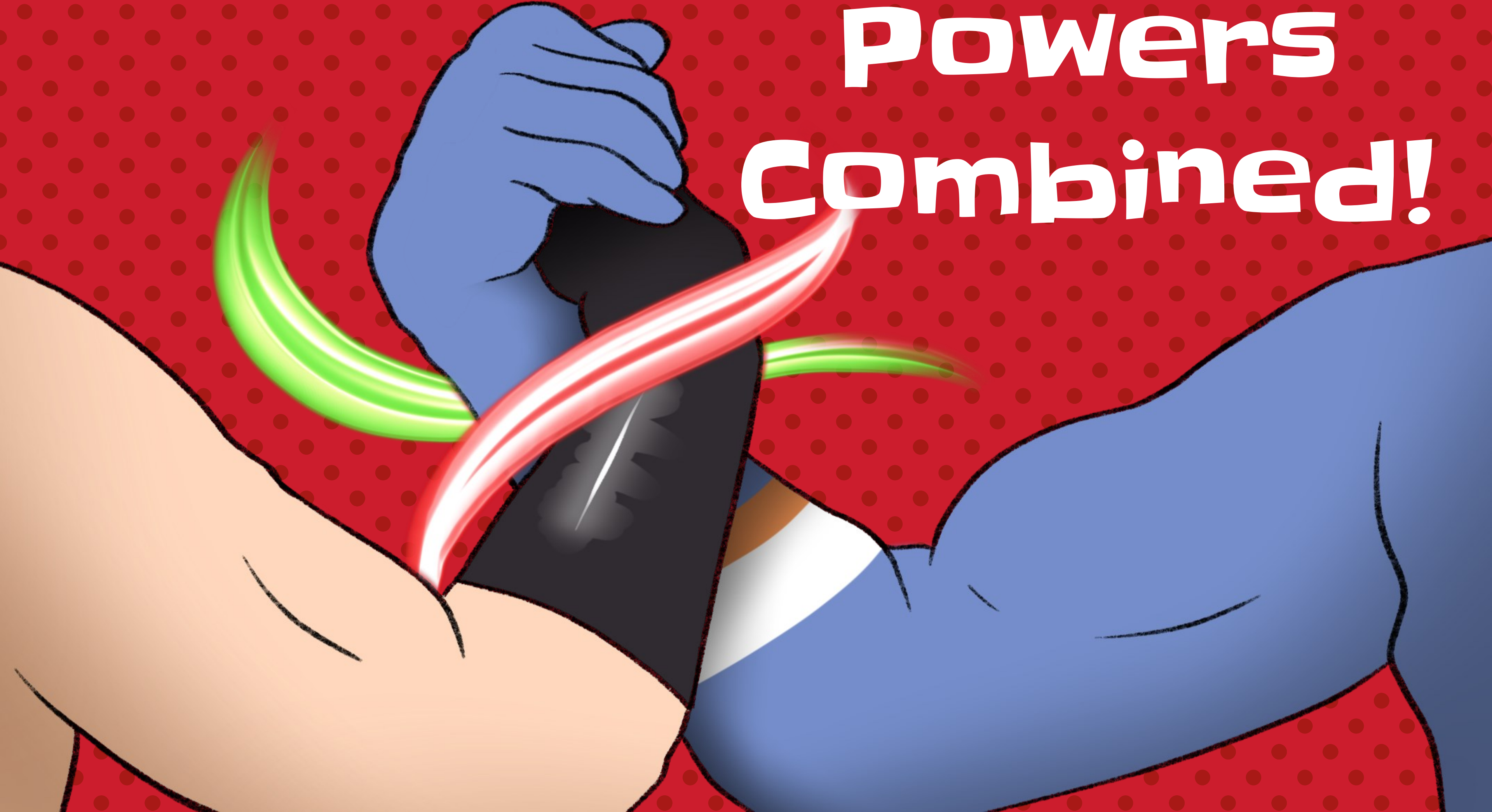
Linking is especially easy for authenticated users, as all requests in the same session are linked.

The use of unique identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data linked to this profile. This can later lead to 'identifying' threats.

www.linddun.org

LINDDUN GO

Powers Combined!



Varied viewpoints

Diverse team for cross-functional collaboration

SECURITY

strengthens privacy

Technical details and attacks

PRIVACY

strengthens security

Logical business flow

User focused = revenue focused

Annotate with Origin Stories

	Security	Privacy
Assets	Kinds of data, Storage technology	More fine grained, Data purpose
Controls	Protocols, encryption, authentication, etc	Access control, consent flows, PETs
Actors	Users, roles, attackers	Individuals, Outsiders, Organization itself

List your Assumptions

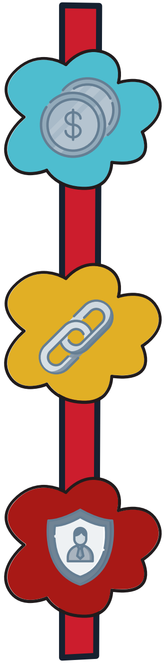
Unanswered questions &
Explicit guesses

Value Driven Threat Modeling

Why?

THE VALUE

Why are we building this?
Why do we need this data?
Why would users care?



How?

THE FEATURE

How do we achieve that value?
How does the value chain work?

What?

COUNTERMEASURES

What do we need to do to fix the chain & and ensure the value?

With
great Privacy
comes
great Security

Epilogue!

Threat Model Everything

Prioritize Privacy

Security + Privacy Together

Secret Identities

Not really a Professor!

Not really a Captain!

Dr. Kim Wuyts

Senior Researcher at
DIstriNet, KU Leuven
Creator of **LINDDUN**

Co-author **Threat
Modeling Manifesto**

Avi Douglen

CEO **Bounce Security**
Vice-Chair at **OWASP**

Thanks for listening, true believers!

Excelsior!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik** and illustrations by **Storyset** Superhero artwork by **Sam Vercammen**, Costuming and flair by **Emette Ahava**.