SPARTA

Security & Privacy Architecture through Risk-driven Threat Assessment

Insecure design in OWASP top 10

“[...], we need more threat modeling, secure design patterns and principles, and reference architectures. [...]”

Top 10 2021

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

Insecure design in OWASP top 10

“[…], we need more threat modeling, secure design patterns and principles, and reference architectures. […]”

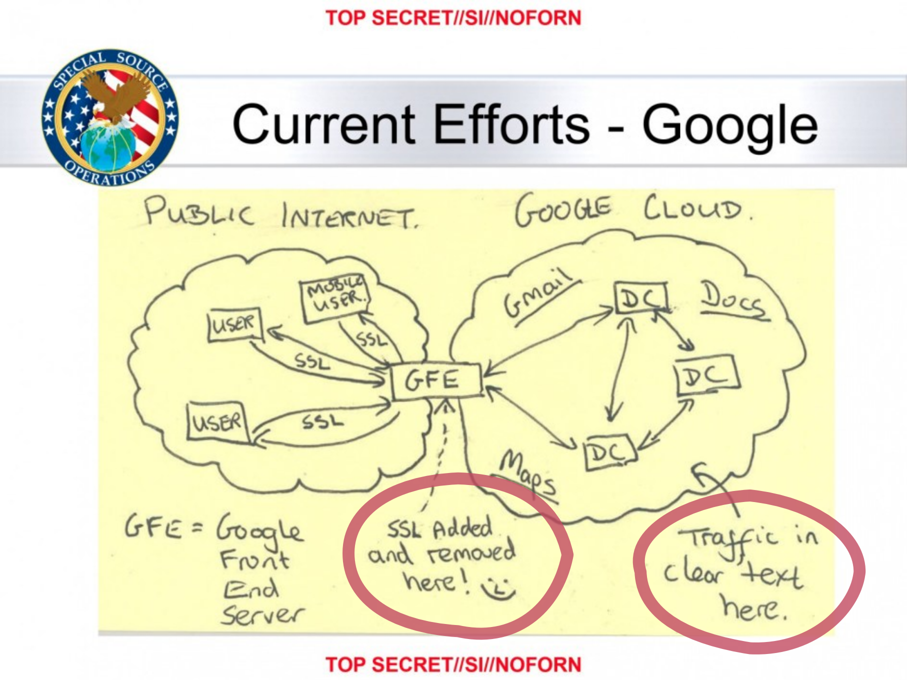
Top 10 2021

A01 Broken Access Control
A02 Cryptographic Failures
A03 Injection
A04 Insecure Design
A05 Security Misconfiguration
A06 Vulnerable and Outdated Components
A07 Identification and Authentication Failures
A08 Software and Data Integrity Failures
A09 Security Logging and Monitoring Failures
A10 Server Side Request Forgery (SSRF)

Consider the security of your design up-front

Analyze your design for security

Because your adversaries certainly do



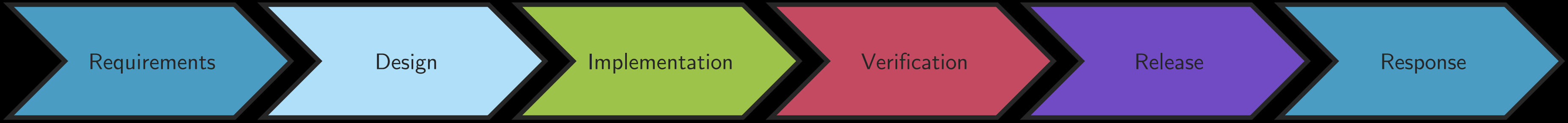
TOP SECRET//SI//NOFORN

Current Efforts - Google

SPECIAL SOURCE OPERATIONS
PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER
USER
SSL
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

TOP SECRET//SI//NOFORN

Tackling security early in the development lifecycle



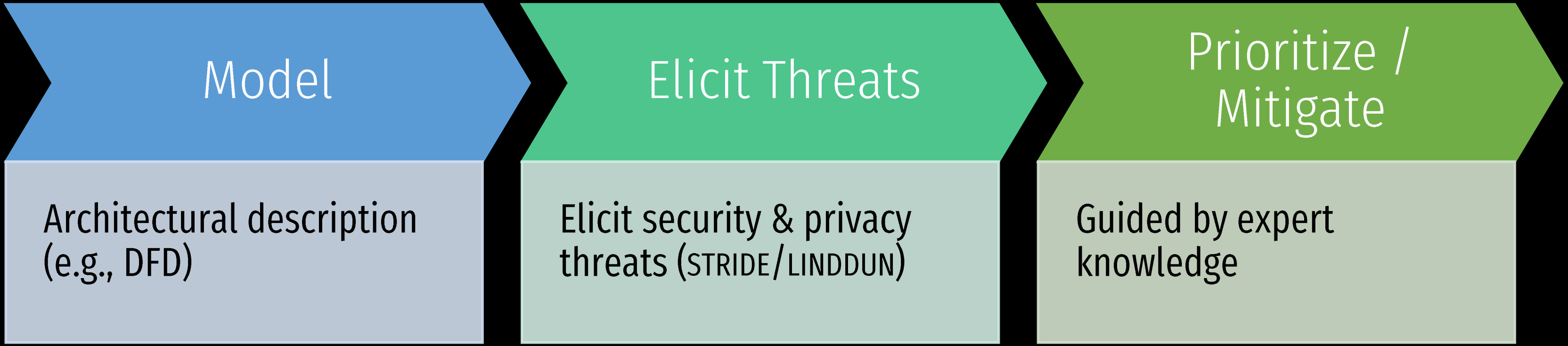
Early analysis

Perform analysis to identify threats in the early stages of development

Feedback-loop

Continuously re-assess the impact of changes as they are made

Threat Modeling Process



Model

Architectural description (e.g., DFD)

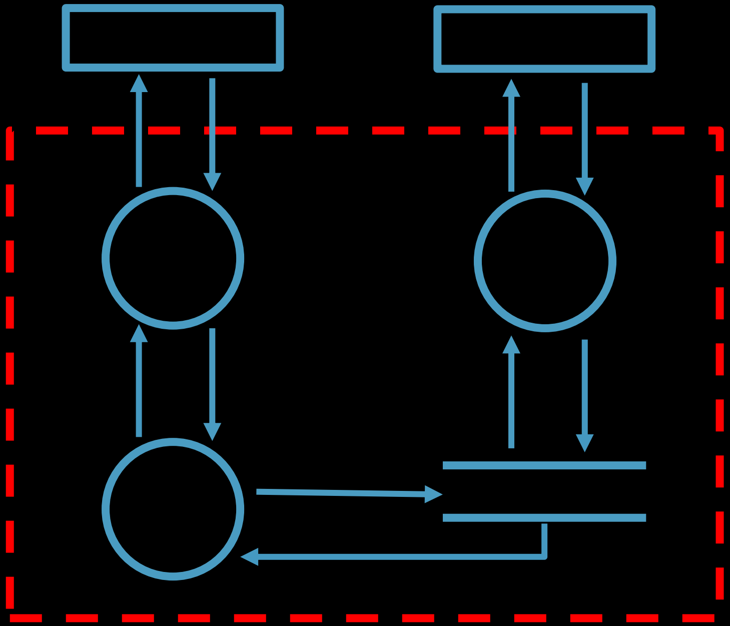
Elicit Threats

Elicit security & privacy threats (STRIDE/LINDDUN)

Prioritize / Mitigate

Guided by expert knowledge

Problem: automation is hindered by lack of support for security and privacy in generic DFDS



No solutions

Except in an ad hoc fashion

No assets

E.g., personal information, cryptographic keys

No prioritization

Lacking support to prioritize threats

Threat modeling with SPARTA

Extended DFD models

First-class support for security and privacy solutions

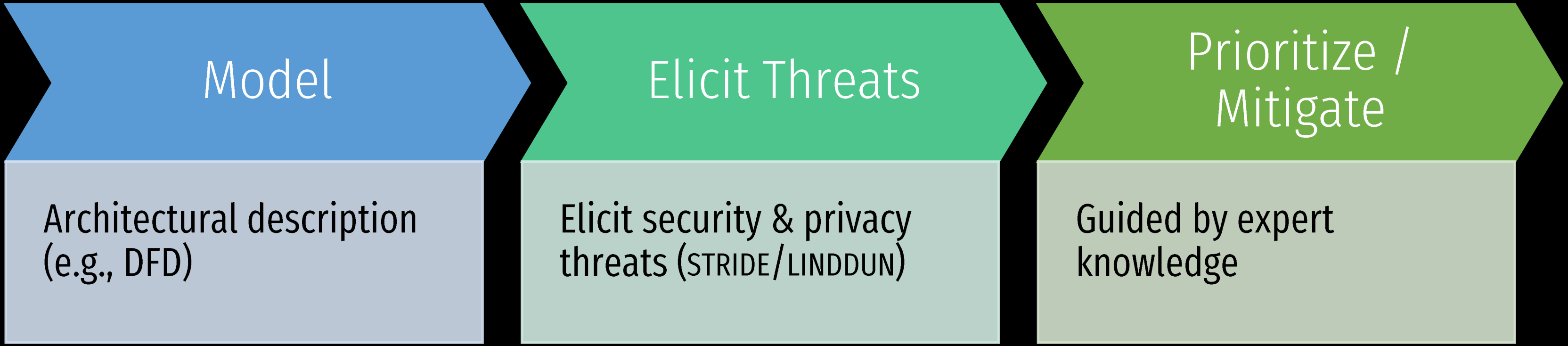
Risk-driven prioritization

Prioritize elicited security and privacy threats

Automation

Continuously re-assess while models are updated

SPARTA improvements



Model

Architectural description (e.g., DFD)

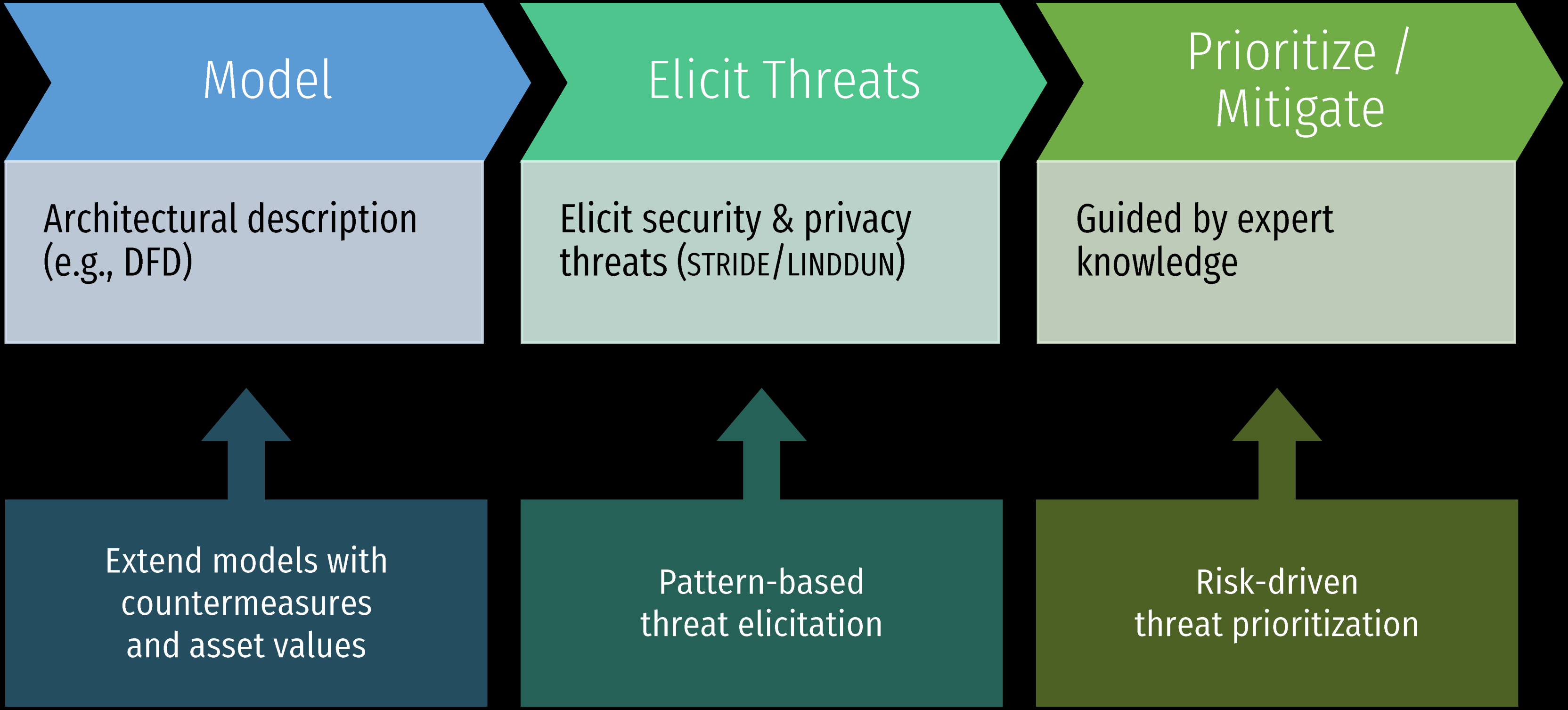
Elicit Threats

Elicit security & privacy threats (STRIDE/LINDDUN)

Prioritize / Mitigate

Guided by expert knowledge

SPARTA improvements



Model

Architectural description (e.g., DFD)

Elicit Threats

Elicit security & privacy threats (STRIDE/LINDDUN)

Prioritize / Mitigate

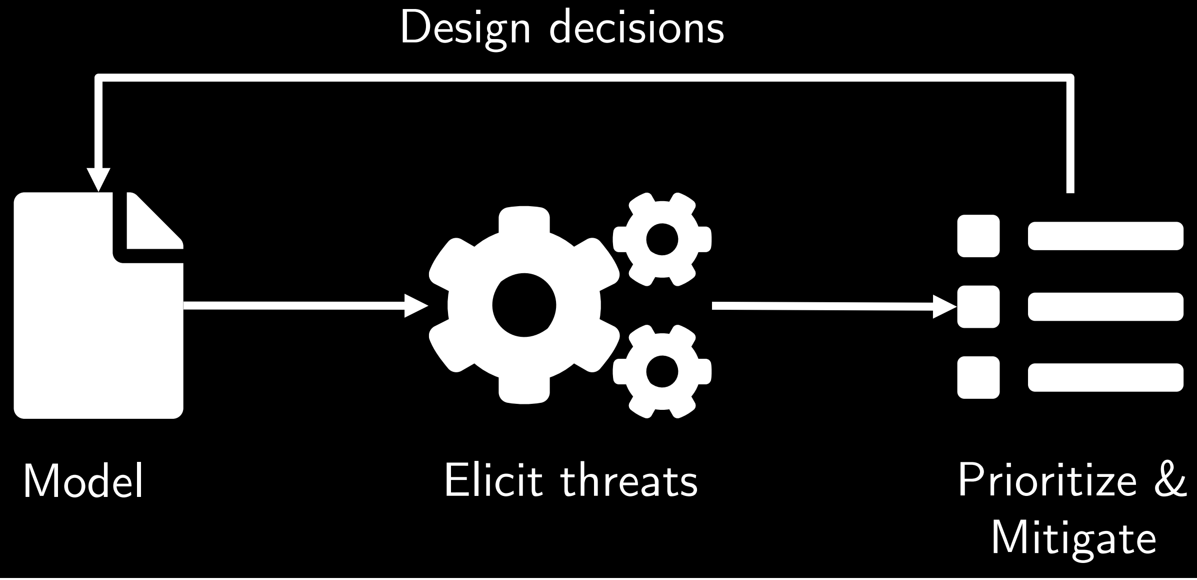
Guided by expert knowledge

Extend models with countermeasures and asset values

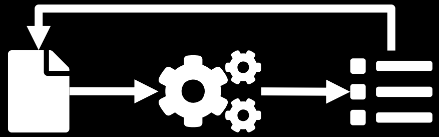
Pattern-based threat elicitation

Risk-driven threat prioritization

Sparta Approach


Design decisions
Model
Elicit threats
Prioritize &
Mitigate

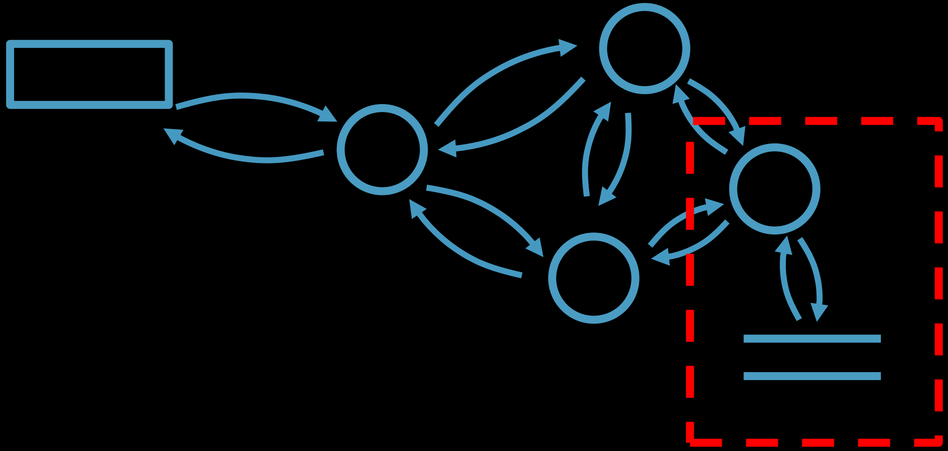
SPARTA



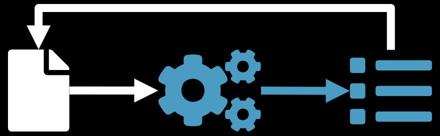
Modeling the system

Construct model of the system

Processes, data flows, external entities, data stores, trust boundaries



Elicit threats



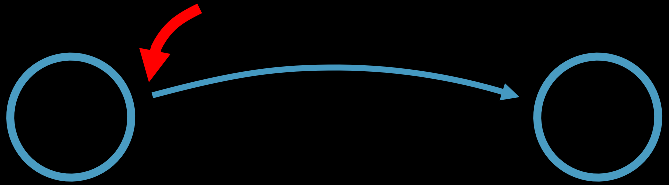
Construct model of the system

Processes, data flows, external entities, data stores, trust boundaries

Analyze model

Iterate over every interaction to identify threats

E.g., spoofing the sender



Apply mitigations

Construct model of the system

Processes, data flows, external entities, data stores, trust boundaries

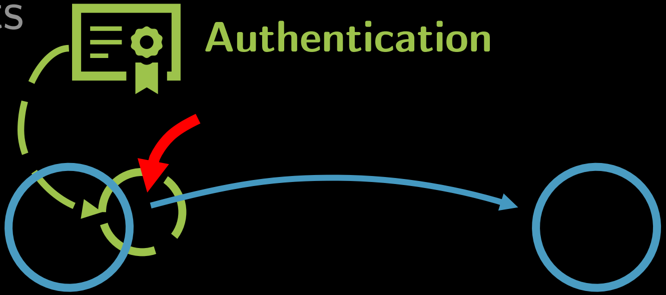
Analyze model

Iterate over every interaction to identify threats

E.g., spoofing the sender

Mitigate threats

E.g., apply authentication



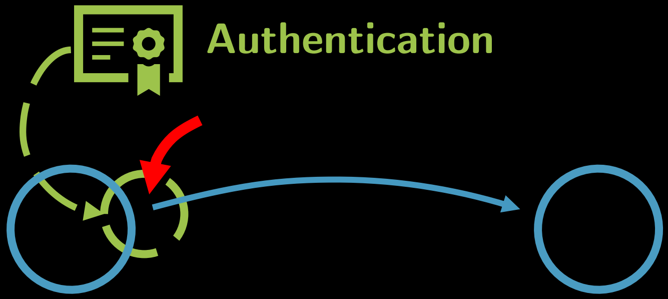
Re-assess

Mitigate threats

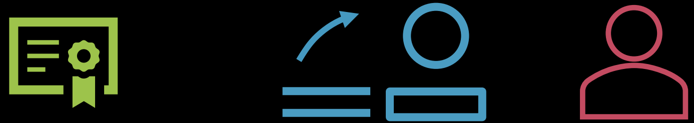
E.g., apply authentication

Analysis takes into account the mitigations

Risk analysis considering countermeasures, asset values, attacker model



Authentication

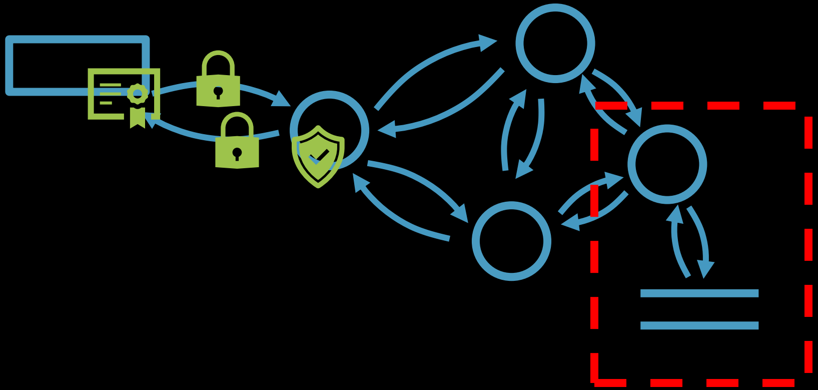


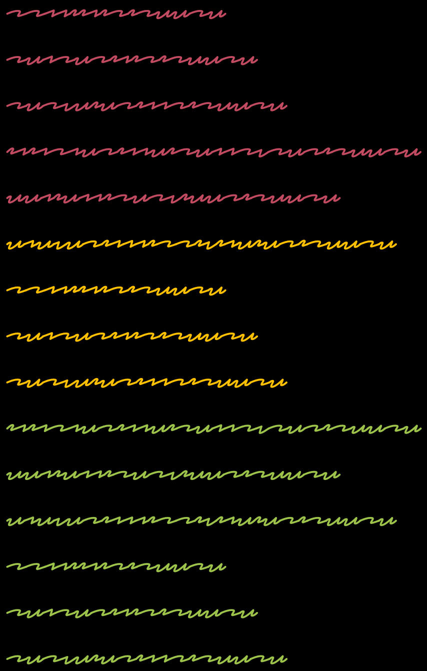
Countermeasure strength

Asset value

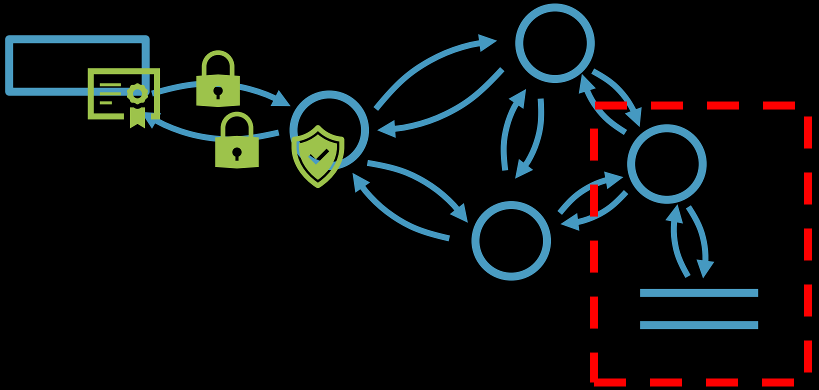
Attacker model

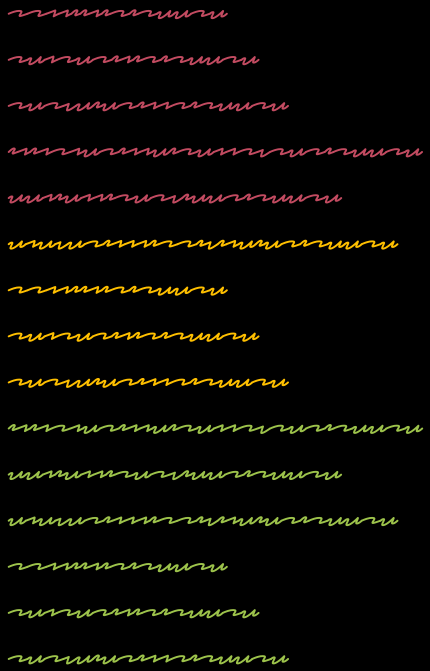
As solutions are added…



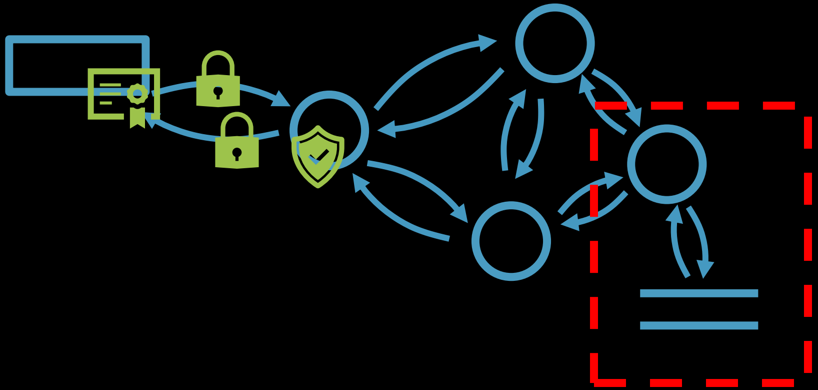


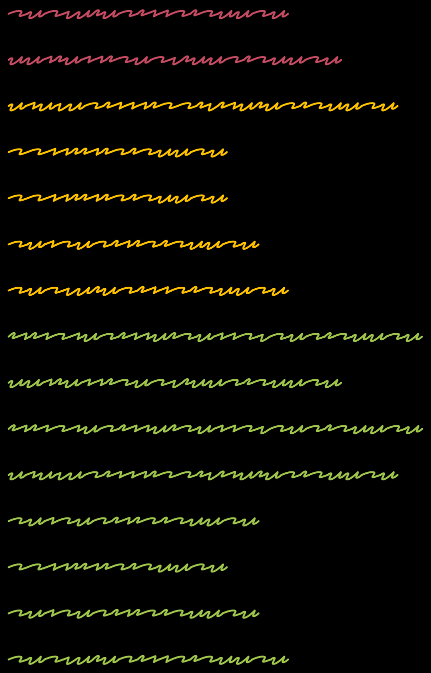
Threats are re-prioritized



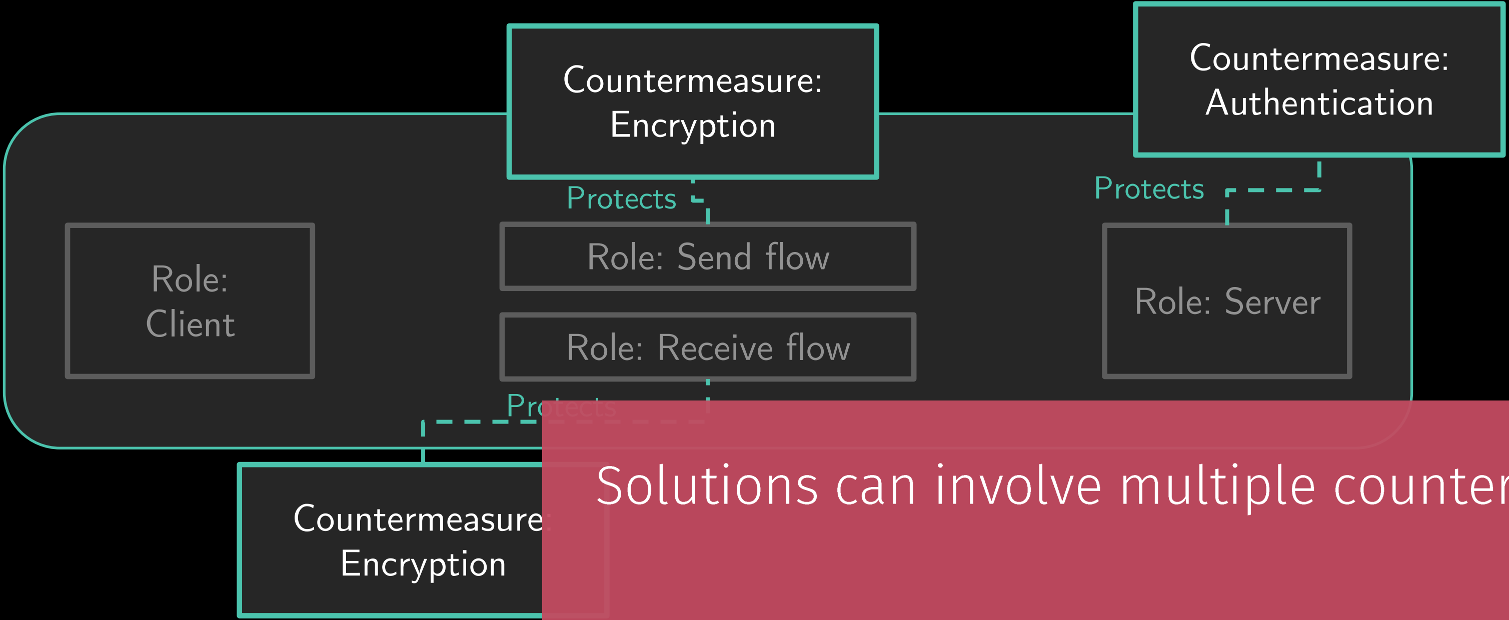


Threats are re-prioritized

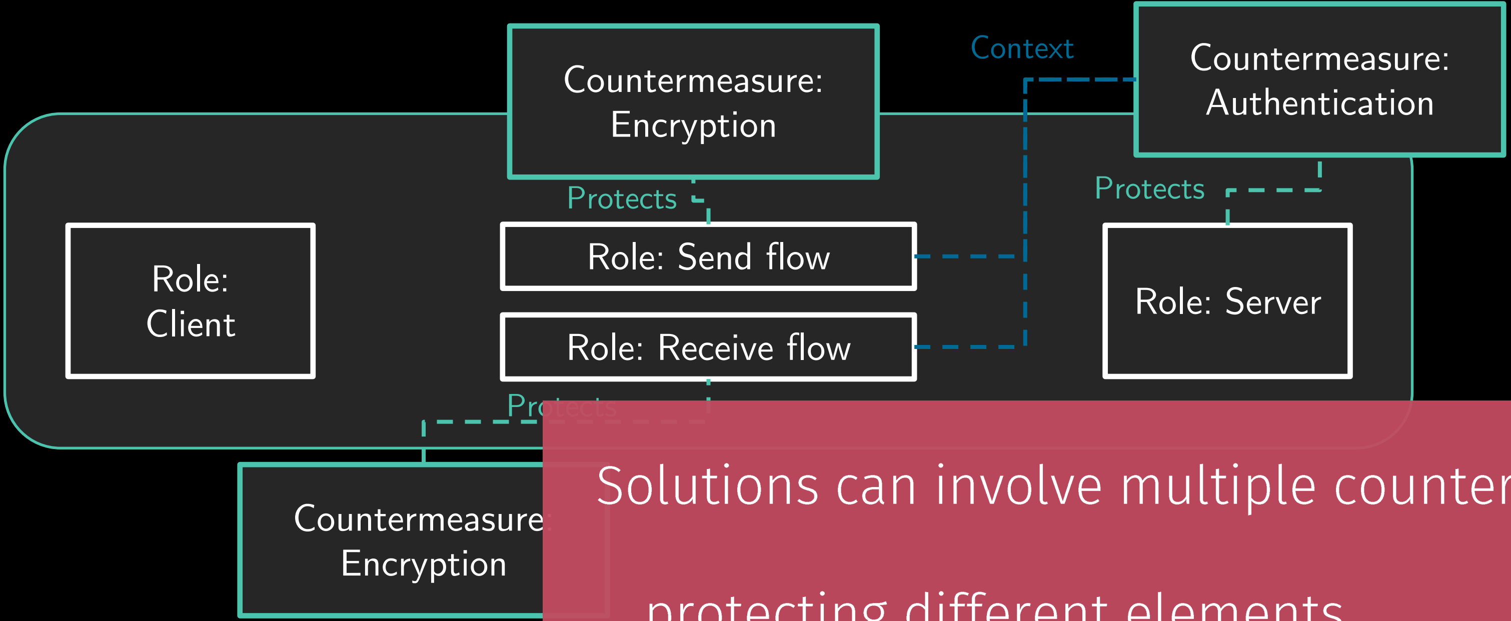




Security & privacy solutions

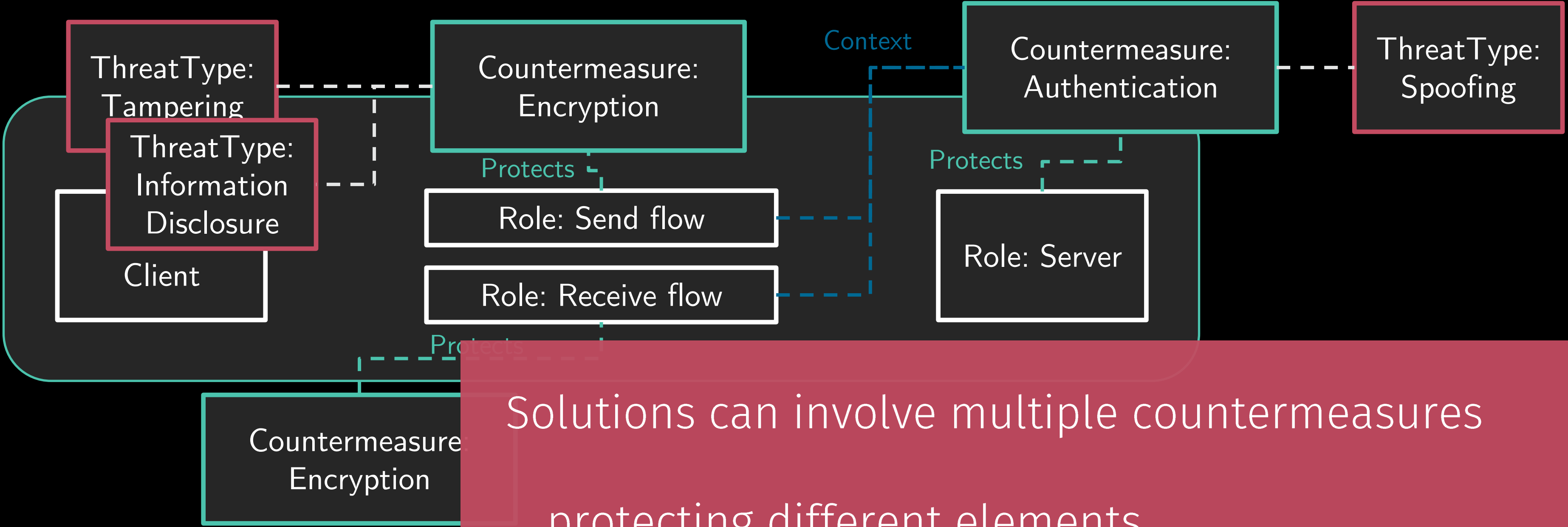


Solutions can involve multiple countermeasures



Solutions can involve multiple countermeasures

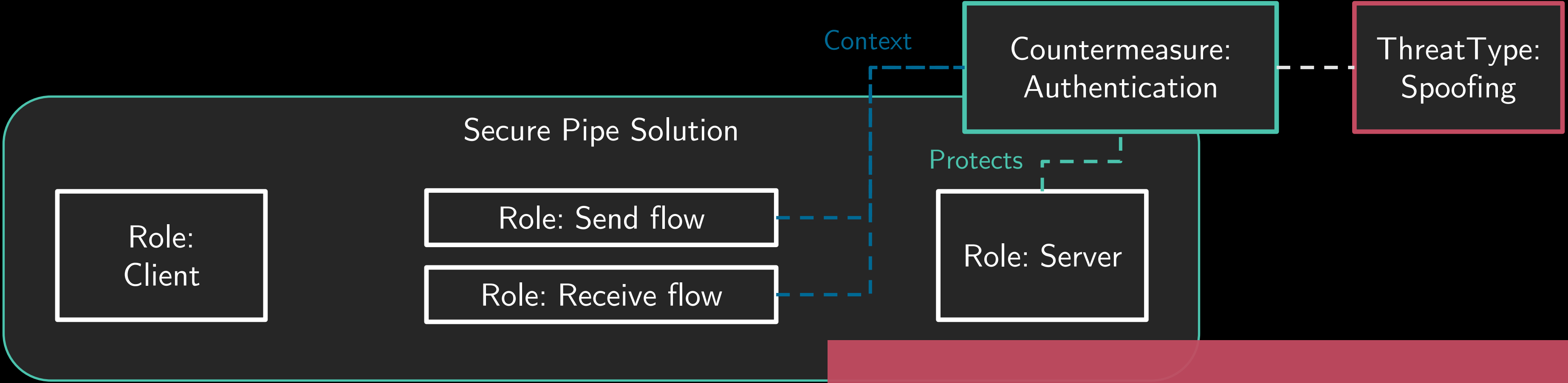
... protecting different elements



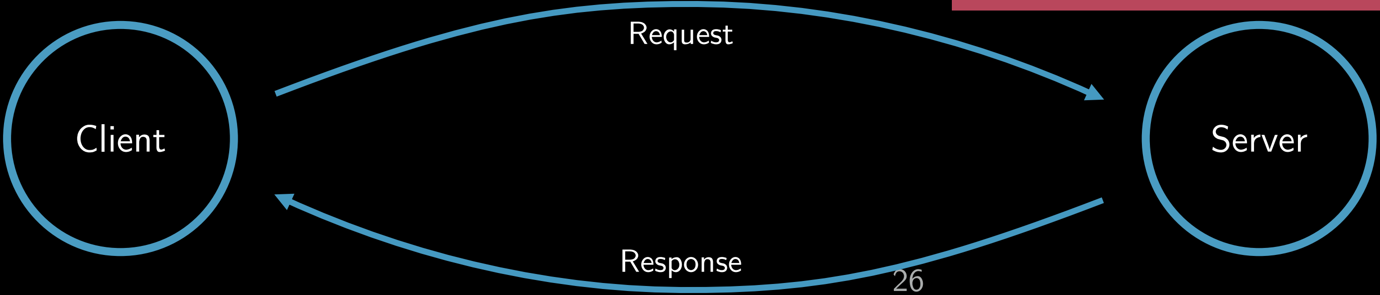
Solutions can involve multiple countermeasures

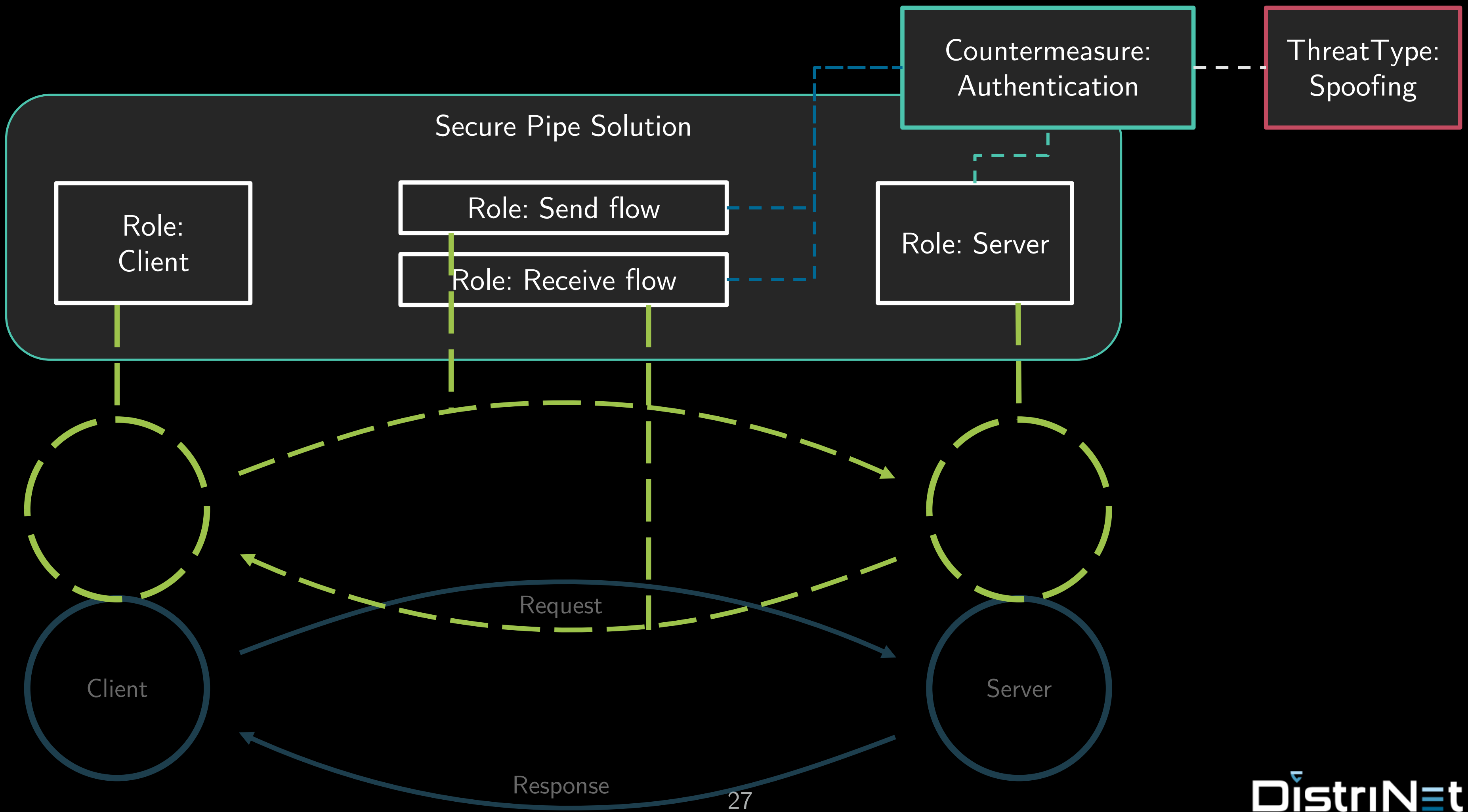
… protecting different elements

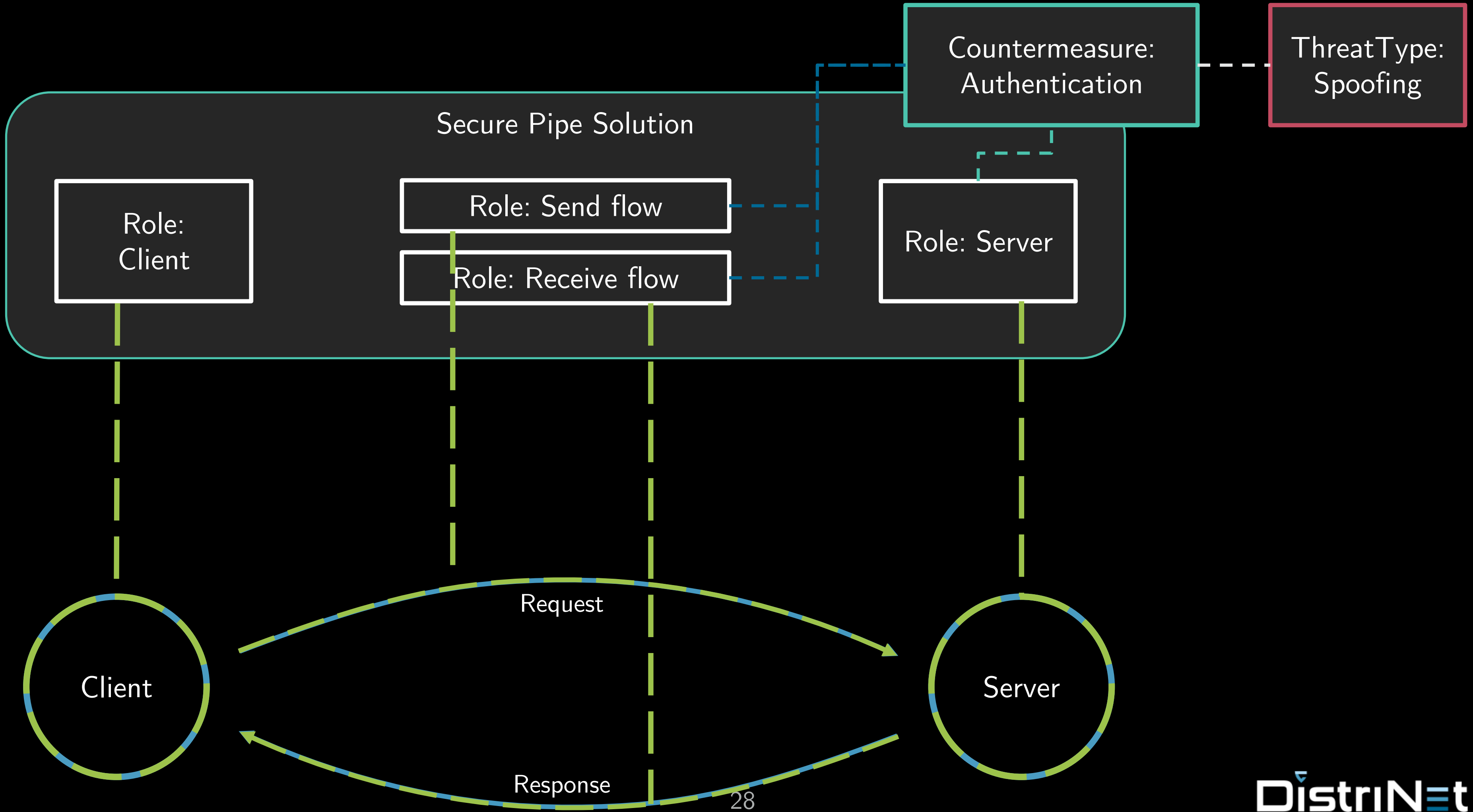
… protecting against different types of threats



... reusable in multiple locations

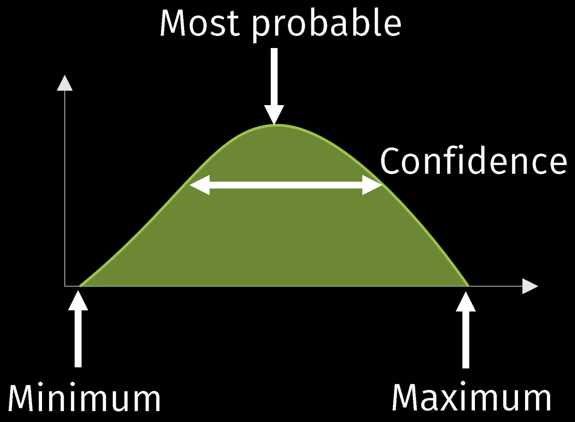


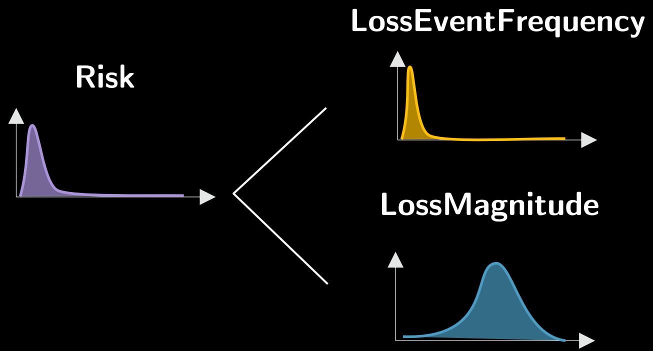

Countermeasure: Authentication
ThreatType: Spoofing
Secure Pipe Solution
Role: Client
Role: Send flow
Role: Receive flow
Role: Server
Request
Client
Server
Response


Countermeasure: Authentication
ThreatType: Spoofing
Secure Pipe Solution
Role: Client
Role: Send flow
Role: Receive flow
Role: Server
Client
Request
Response
Server

Risk-driven threat prioritization

Prioritizing threats using risk indicators





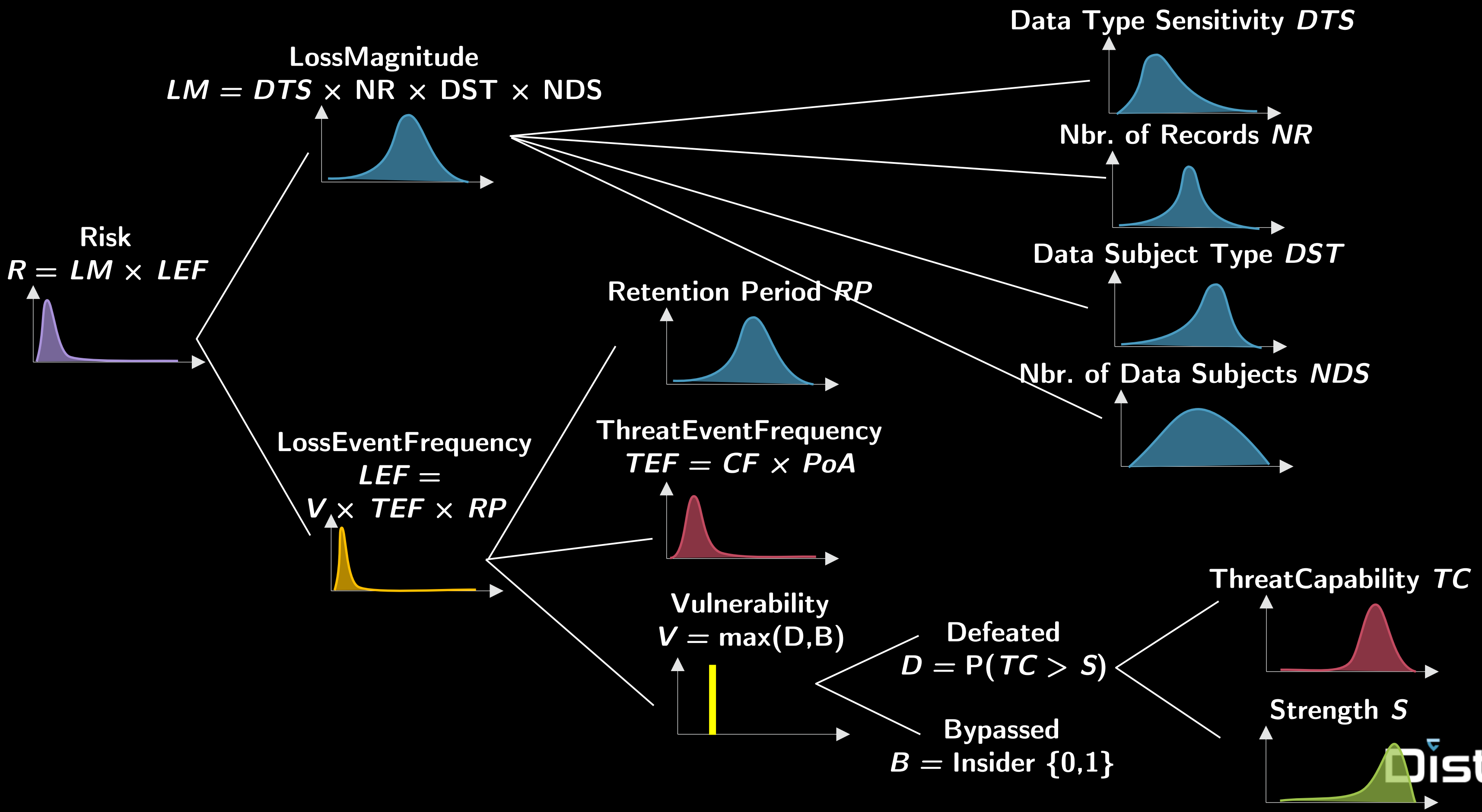
Inputs are estimates

Represents distribution to sample from

Inputs belong to one of 5 categories

System, threat type, attacker profile, data subject type, datatype

Detailed risk breakdown calculated per threat



Risk

$R = LM \times LEF$

LossMagnitude

$LM = DTS \times \mathrm{NR} \times \mathrm{DST} \times \mathrm{NDS}$

Data Type Sensitivity DTS

Nbr. of Records NR

Data Subject Type DST

Nbr. of Data Subjects NDS

LossEventFrequency

$LEF =$

$V \times TEF \times RP$

Retention Period RP

ThreatEventFrequency

$TEF = CF \times PoA$

Vulnerability

$V = \max(\mathrm{D,B})$

Defeated

$D = \mathrm{P}(TC > S)$

Bypassed

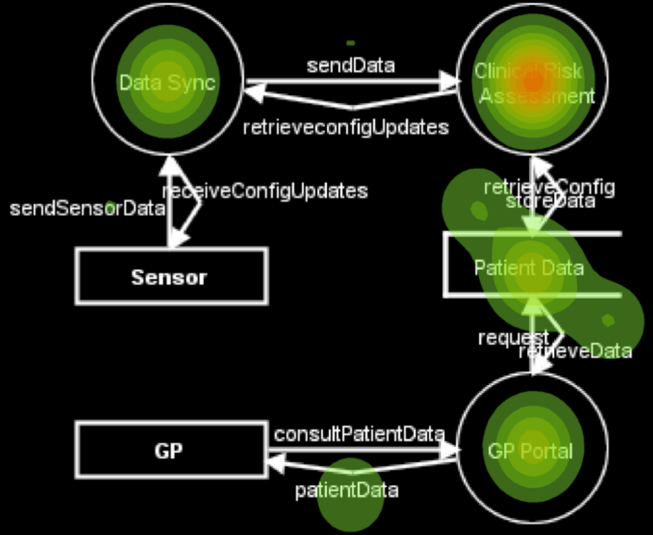
$B = \text{Insider } \{0,1\}$

ThreatCapability TC

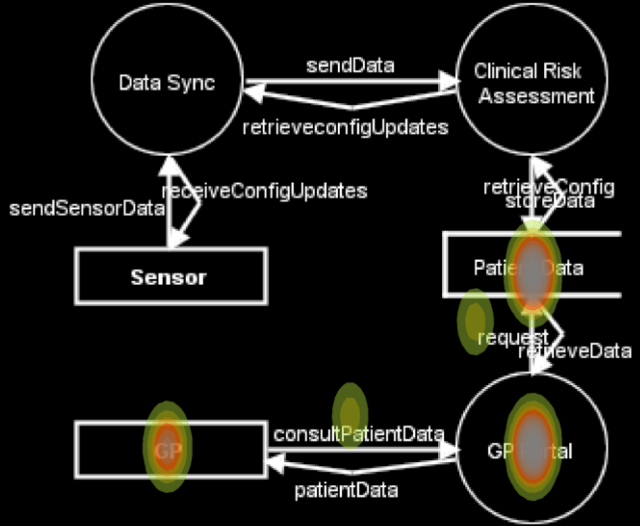
Strength S

Intermediate risk results can be aggregated

For example: per element and data subject type



Patient Risk



General Practitioner Risk

Case study

Evaluation: case study on the SecureDrop whistleblower submission system

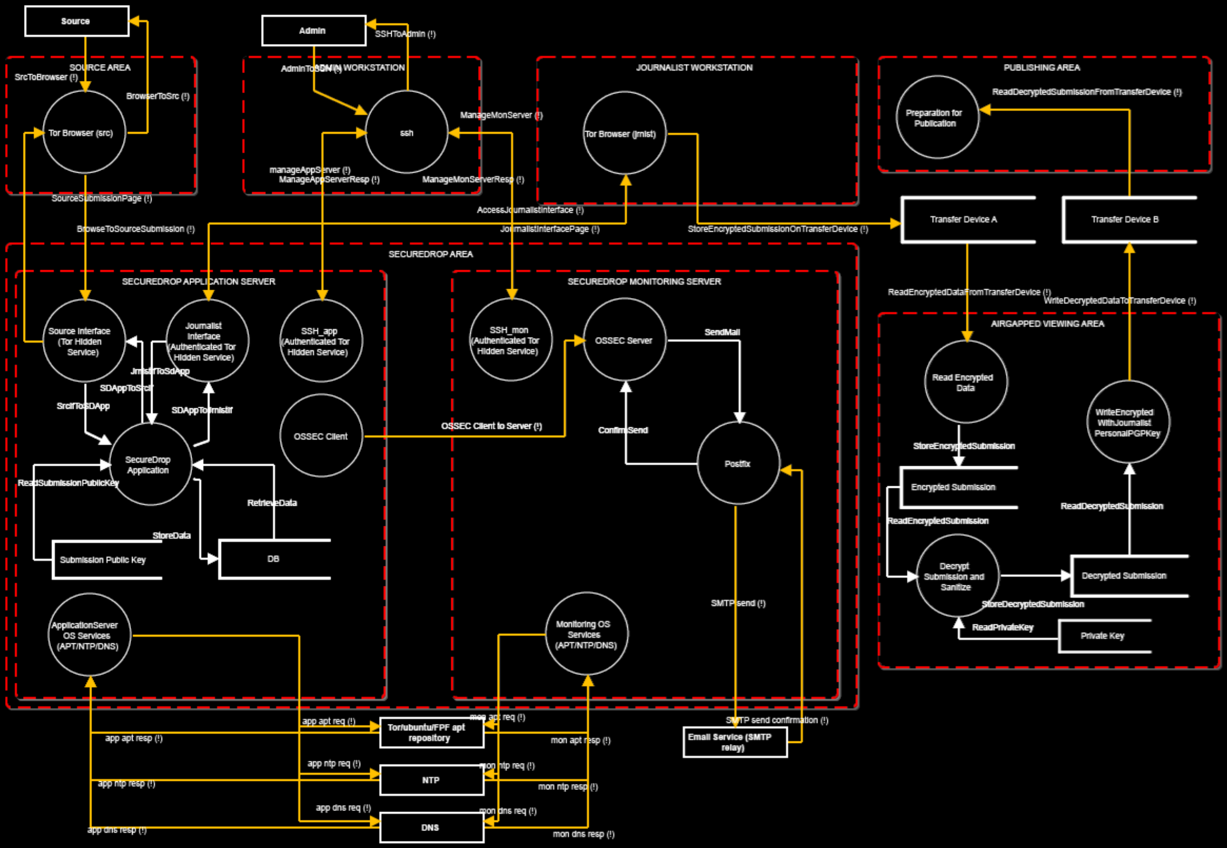
For media organizations

35 instances: Washington Post, New York Times, The Guardian, etc.

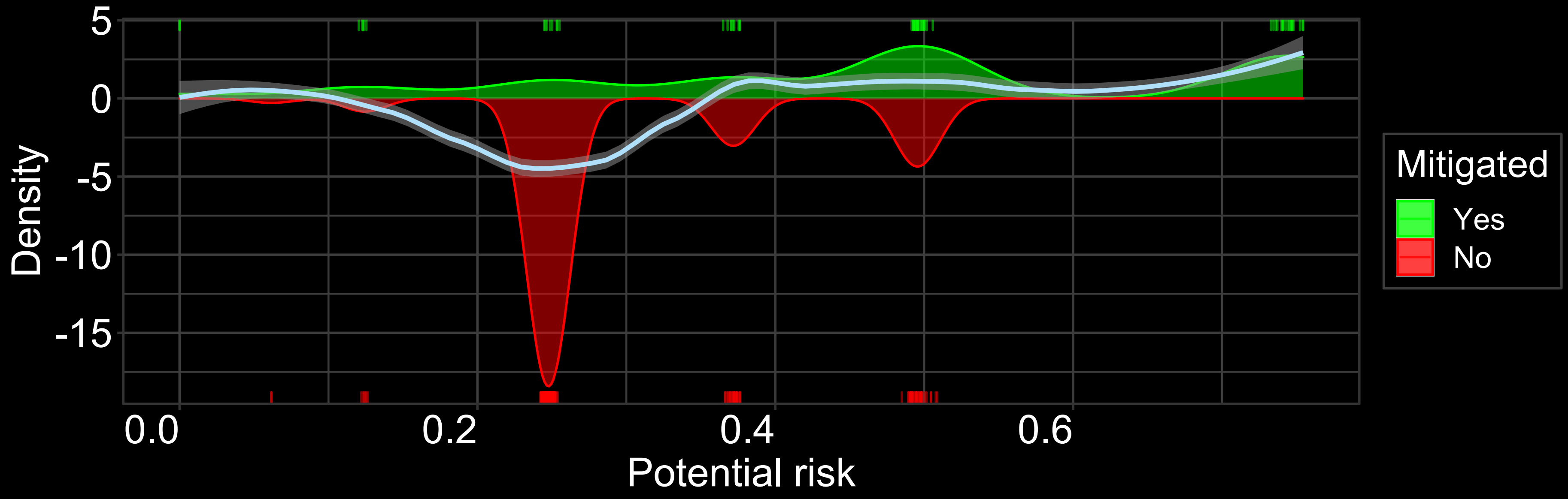
Anonymous journalistic sources

Protecting identity critical

SecureDrop whistleblower submission system



Higher risk threats have mitigations present



Demo

SPARTA: Automation and tool support

Iterative design feedback (early SDLC stages)

Continuous design assessment

Lightweight architectural descriptions

Extended DFDs with security and privacy solution support

Threat elicitation & risk-driven prioritization

FAIR-based risk decomposition

Evaluated feasibility

SecureDrop case study

Sparta framework as a driver for future threat analysis innovations

Extend analysis activities

Leverage relations between threats

Decision support

Evaluation and compare of design decisions

Track threat mitigation evolution during development

Continuous analysis and monitoring of threats

SPARTA

sparta.distrinet-research.be