SV.lu
software verification & validation

SnT
securityandtrust.lu

Secure and Compliant Data Management in FinTech Applications

Prof. Lionel Briand, FNR PEARL Chair

UL 3X3 FinTech lecture series, February 10th, 2017

uni.lu
UNIVERSITÉ DU LUXEMBOURG

FinTech @ SnT Centre

- **SnT:** Luxembourg's center on ICT Security, reliability and Trust
- > **260** staff members
- **31** partners
- **FinTech:** One of SnT's priorities
- **Increasing momentum:** 5 FinTech partners, 7 projects, 2 laboratories

Alphonse Weicker Foundation

Software Verification and Validation @ SnT

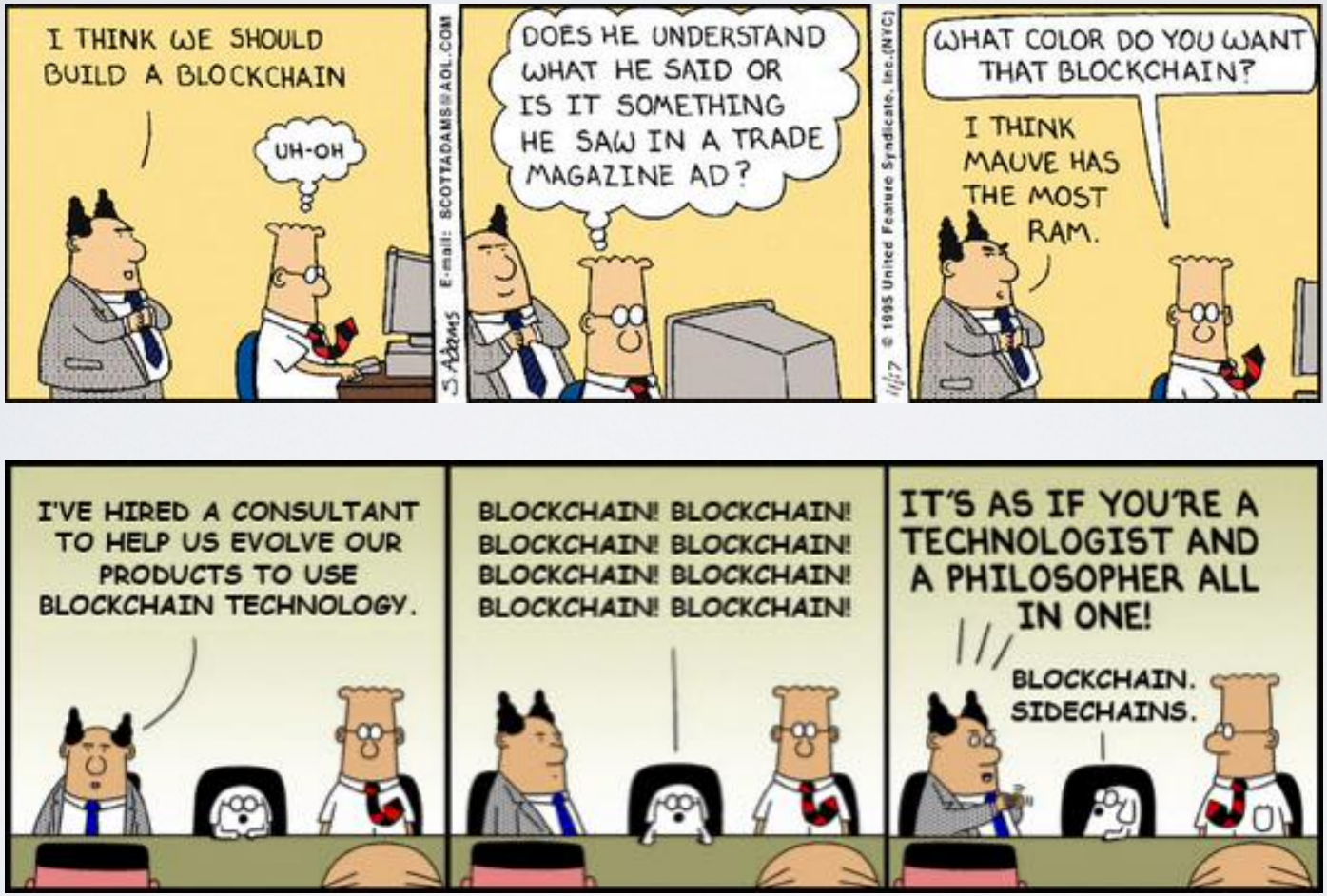
- Group established in 2012 (FNR PEARL)
- **Focus:** Ensuring reliability and security of IT systems through automated, cost-effective V&V solutions, e.g., testing
- ERC Advanced Grant
- ~ 25 staff members
- Industry partnerships

Objectives

- Create awareness about the challenges and solutions for ensuring secure and compliant data management in FinTech applications
- Motivate the need for research and innovation
- Non-technical presentation
- Not meant to be a complete treatment of the subject matter

FinTech

Not Just about the B Word



FinTech: State of Play

- **$14.5 billion globally** in venture capital in 2015, from $7.3 billion in 2014
- FinTech companies are **proliferating**
- Wide range of solutions that promise to **impact nearly everyone**
- Dramatically broaden the **reach, flexibility, and level of innovation** of financial services
- Key challenge: **Cybersecurity**
- **Risks:** Financial losses, undermine confidence, lower adoption

Cybersecurity: Risk Factors

- "All that matters is to get to market fast" mentality
- **Growing mismatch** between technology and regulations
- **Dilemma:** Consumer protection versus the agility of the innovation ecosystem

Cybersecurity: Risk Factors

- Reliance on **machine learning** and big data complicates the picture regarding cybersecurity – unintended biases in system behavior
- Many new "customers" with **little knowledge** of security risks
- **More interfaces** between traditional financial services and FinTech applications

Did I manage to worry you?

How Secure is our Data?

N.Y. / REGION

In Hours, Thieves Took $4

04 Thieves Jam Up Smu

MAR 14

Jam and jelly maker **Smucker's** last week shu
site was being retooled because of a security
data. Closer examination of the attack suggests
firms — including at least one credit card proc
gang that infiltrated some of the world's biggest

30 MasterCard, VISA Wa

MAR 12

VISA and **MasterCard** are alerting banks across the cou

Ban

Mike Sn

(Photo: Spe

THE W

Home World U.S. Politics E

Car Insurers Find Tracking Devices Are a Tough Sell

Apple News Is a Rocky Start

TECH

51

CurrentC, Retailers' Tı Hacked

Email Addresses Taken During Pilot Project

NEWS ANALYSIS

European Central Bank hacked

By Brian Honan | Follow

CSO | Jul 31, 2015 8:22 AM PT

RELATED TOPICS

Data Breach

1 COMMENT

INSIDER

The European Central Bank (the ECB) announced on Thursday the 24th of July that its website was the victim of a cyber-attack resulting in the security of the site being compromised. The attack resulted in a breach of the security for a database serving its public website. The database is

JPMorgan Chase Data Breach (2014)

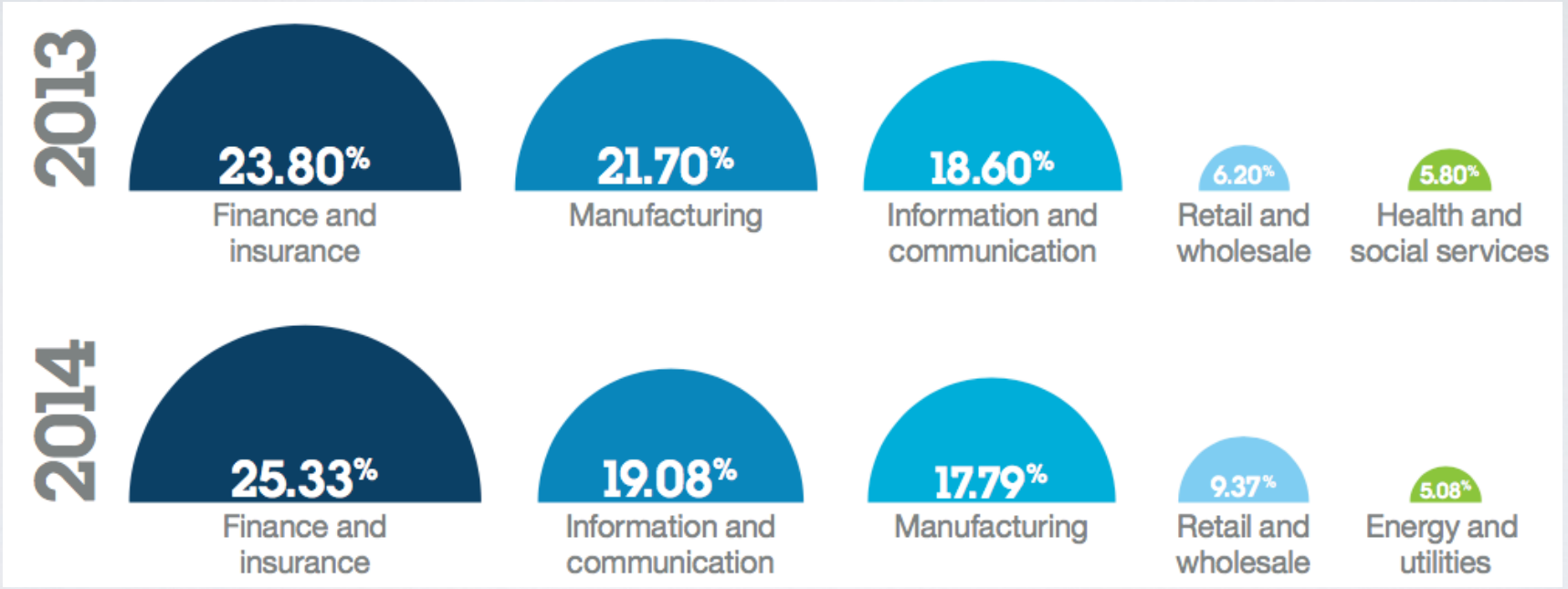
- Compromised over 83 million accounts - 76 million households and 7 million small businesses
- Also, targeted 9 other major financial institutions alongside JPMorgan Chase

UK's Tesco Bank Hack in Nov 2016

- Biggest cyber attack in the history of British banking
- **£2.5 million** stolen from accounts of **9000** customers
- Approximately **40,000** Tesco Bank accounts were compromised
- The fine could be as much as **£2 billion** pounds under the GDPR rules.

Some Statistics about Cybersecurity

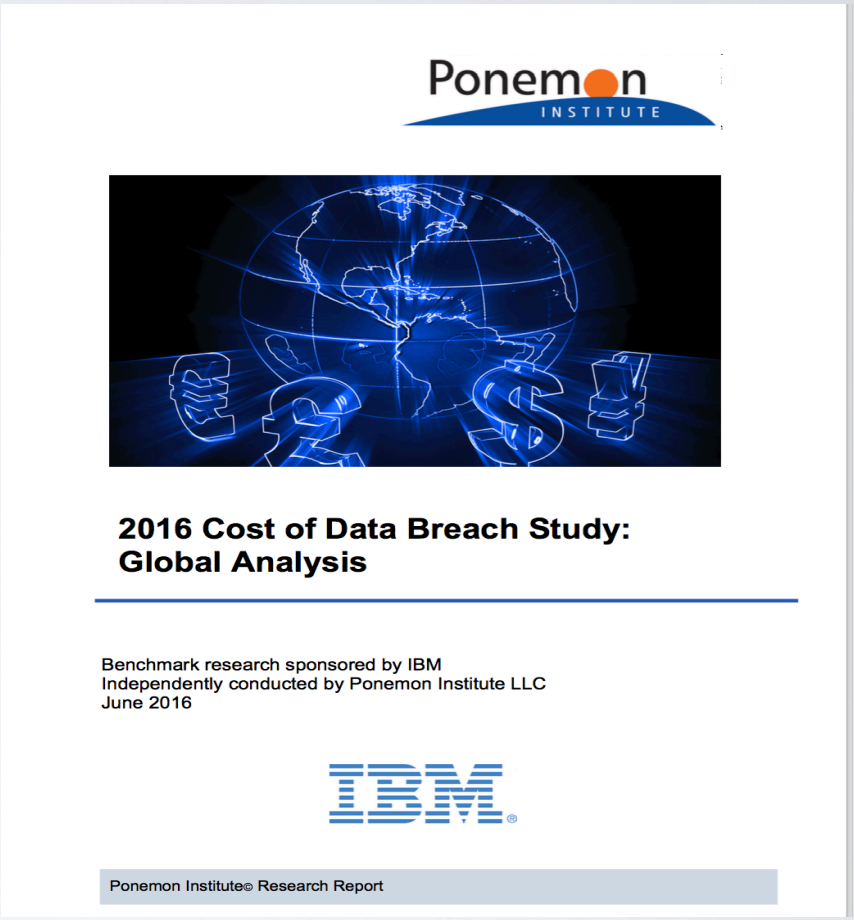
Incident rates by industries



Source: IBM Security - data from worldwide organisations having between 1,000 and 5,000 employees

Financial Impact of Data Breaches

- Study of **383** companies in **12** countries
- **$4** million is the average total cost of a data breach
- **29%** increase in total cost of data breach since 2013
- **$158** is the average cost per lost or stolen record
- **15%** increase in per capita cost since 2013



Are FinTech Applications Different?

- Most FinTech applications are **web applications or services**, possibly with a mobile front end – they are subject to the **same security challenges** as many other systems
- FinTech applications handle **sensitive data** and perform **business-critical operations**
- For now transactions are relatively limited, but **risk factors are even more acute** than in traditional financial services

BLOCKCHAIN GRAVEYARD

STARTING A BTC/ETH COMPANY?

These cryptocurrency institutions have suffered intrusions resulting in stolen financials, or shutdown of the product. Nearly all closed down afterward.

Nearly every attack could have been prevented:

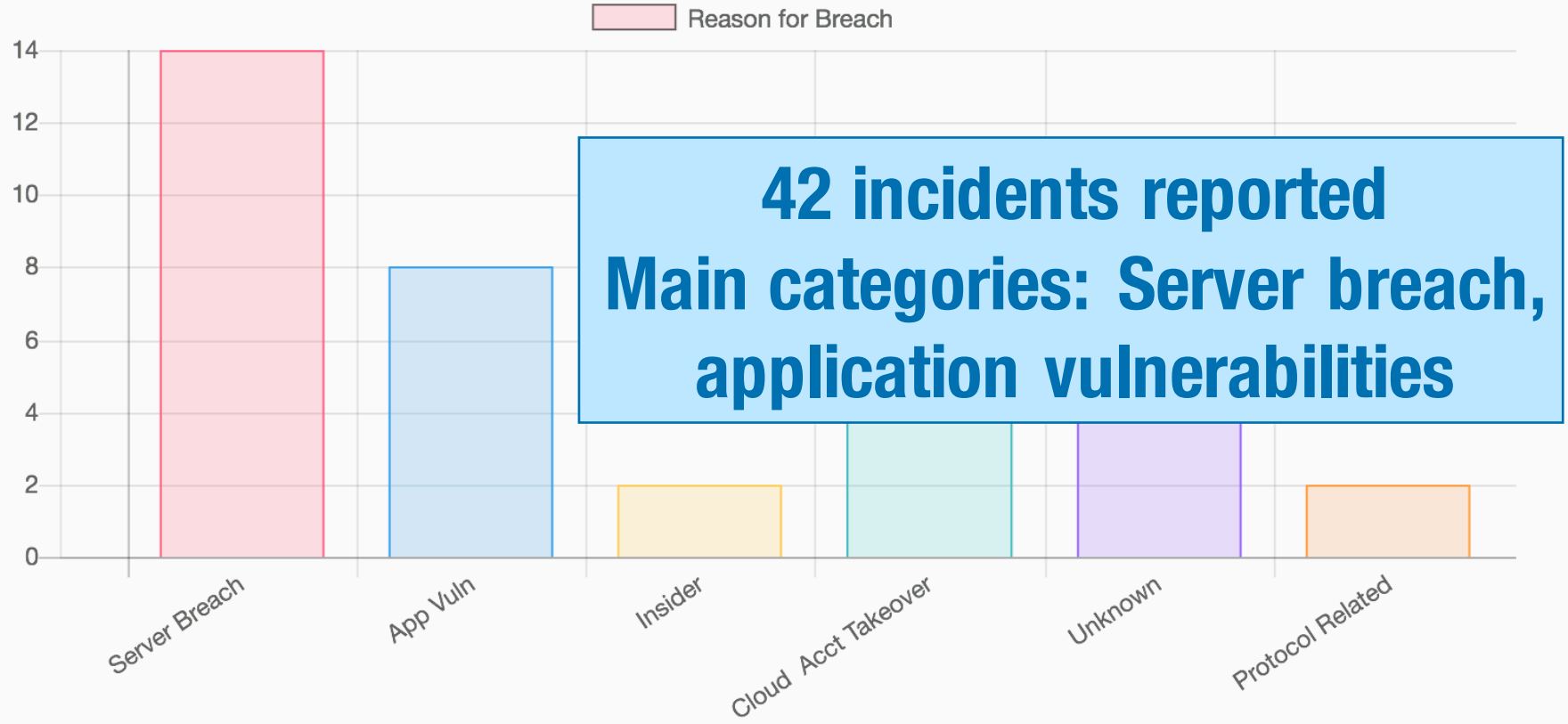
- Social Engineering / Credential Reuse
- Account Takeover of Cloud Hosting
- Application Vulnerability

Each root cause is below, with a link to more information in the breach.

https://magoo.github.io/Blockchain-Graveyard/

ROOT CAUSE ESTIMATES

The data below is roughly gleaned from publicly available data about **42** incidents.



COINWALLET

Application vulnerability due to a lack of input sanitation, type unknown, though it does reference a "database call" which implies some form of database injection like SQLi.

Strangely, they claim that no coins were lost, though CoinWallet shut down anyway.

> It is with great regret that we announce the closure of CoinWallet.co. Our decision to close is based on

Vulnerability: Database injection

Consequence: Data breach

Conclusion: "This incident prompted us to reassess the viability of running coinwallet.co and it was decided it is just not viable taking into consideration the risk, costs and time involved."

> This incident prompted us to reassess the viability of running coinwallet.co and it was decided it is just not viable taking into consideration the risk, costs and time involved.

Summary

- FinTech applications handle sensitive user and corporate data
- Data breaches can ruin a FinTech company's reputation and lead to significant financial damages and legal problems
- FinTech applications must be secure from a data management point of view
- Regulations are becoming more stringent, including the GDPR European legislation on data privacy

Secure data management cannot be ensured during development

- Root causes
  - time to market pressures,
  - lack of disciplined programming,
  - third-party solutions (services, components).

Consequences

- Many applications have problems with
  - incomplete or improper security requirements,
  - inadequate security architecture,
  - implementation flaws,
  - lack of systematic and effective testing,
  - …

Compliance with Standards and Regulations

Compliance

Regulations for FinTech domains

microfinance, crowdfunding, cashless payment, cryptocurrencies, …

Regulations & Standards for FinTech IT Systems

primarily concerned with data protection and privacy

Example from Payment Services

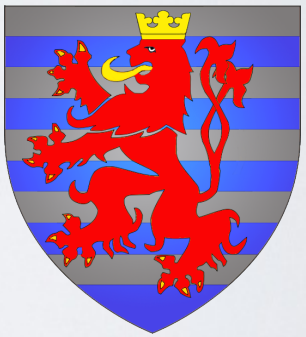
- **PSD2: Payment Services Directive (EU directive)**

- "In order to improve the efficiency of payments throughout the Union, **all payment orders** initiated by the payer and denominated in euro or the currency of a Member State whose currency is not the euro, including credit transfers and money remittances, **should be subject to a maximum 1-day execution time**. For all other payments, such as payments initiated by or through a payee, including direct debits and card payments, in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, **the same 1-day execution time should apply**."

Security and Privacy

- **Security certification**
  - On a voluntary basis
  - Business advantage

- **Laws and regulations**
  - Compliance is mandatory
  - Luxembourg's implementation of EU Directive 95/46/EC
  - General Data Protection Regulation (GDPR)



GDPR

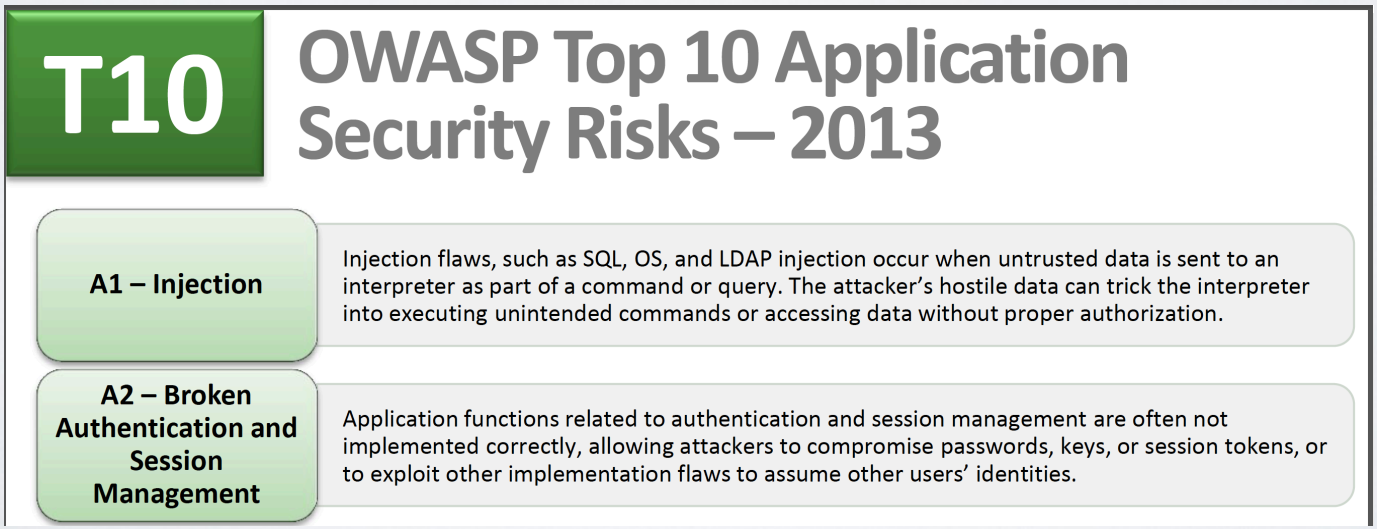
- **Sweeping powers** for national data protection agencies
- Fines of up to 4% of annual turnover for major breaches
- **Major new requirements**, including:
  - Reporting major data breaches within 72h
  - Privacy by design
  - Client's right to be forgotten
- **Verified technical and organizational measures** necessary for demonstrating security

Industry Security Standards

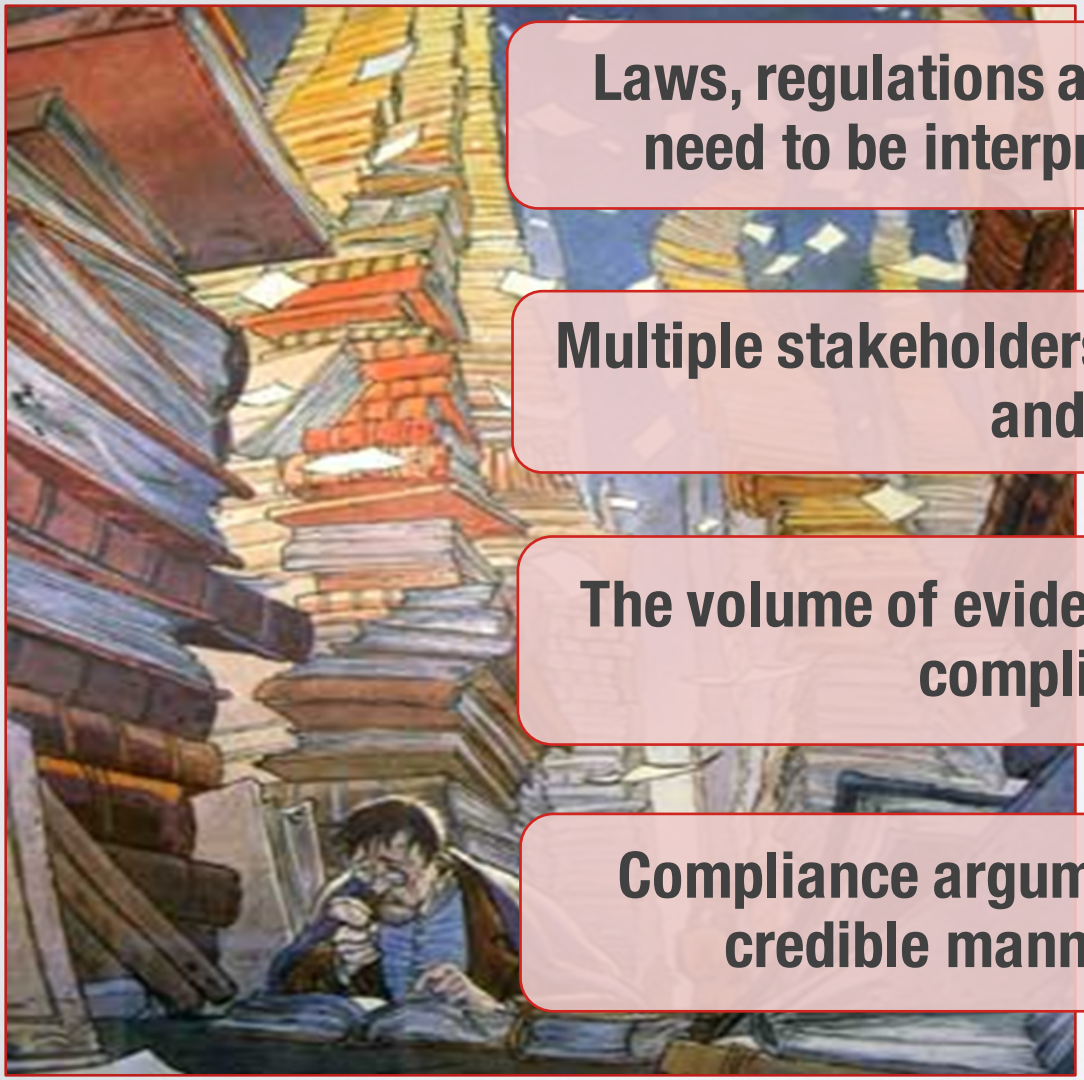
- Payment Card Industry Data Security Standard (PCI DSS)
- Proprietary information and security standard for organizations that handle branded credit cards
- Increase control on credit card data and reduce credit card fraud
- Annual validation of compliance by Qualified Security Assessors

OWASP

- Open Web Application Security Project (OWASP)
- Share relevant software security information and good practices
- https://www.owasp.org/



Compliance is Complex and Expensive



Laws, regulations and standards are textual. They need to be interpreted and adapted to context

Multiple stakeholders are involved in the compliance and auditing chain

The volume of evidence required for demonstrating compliance is very large

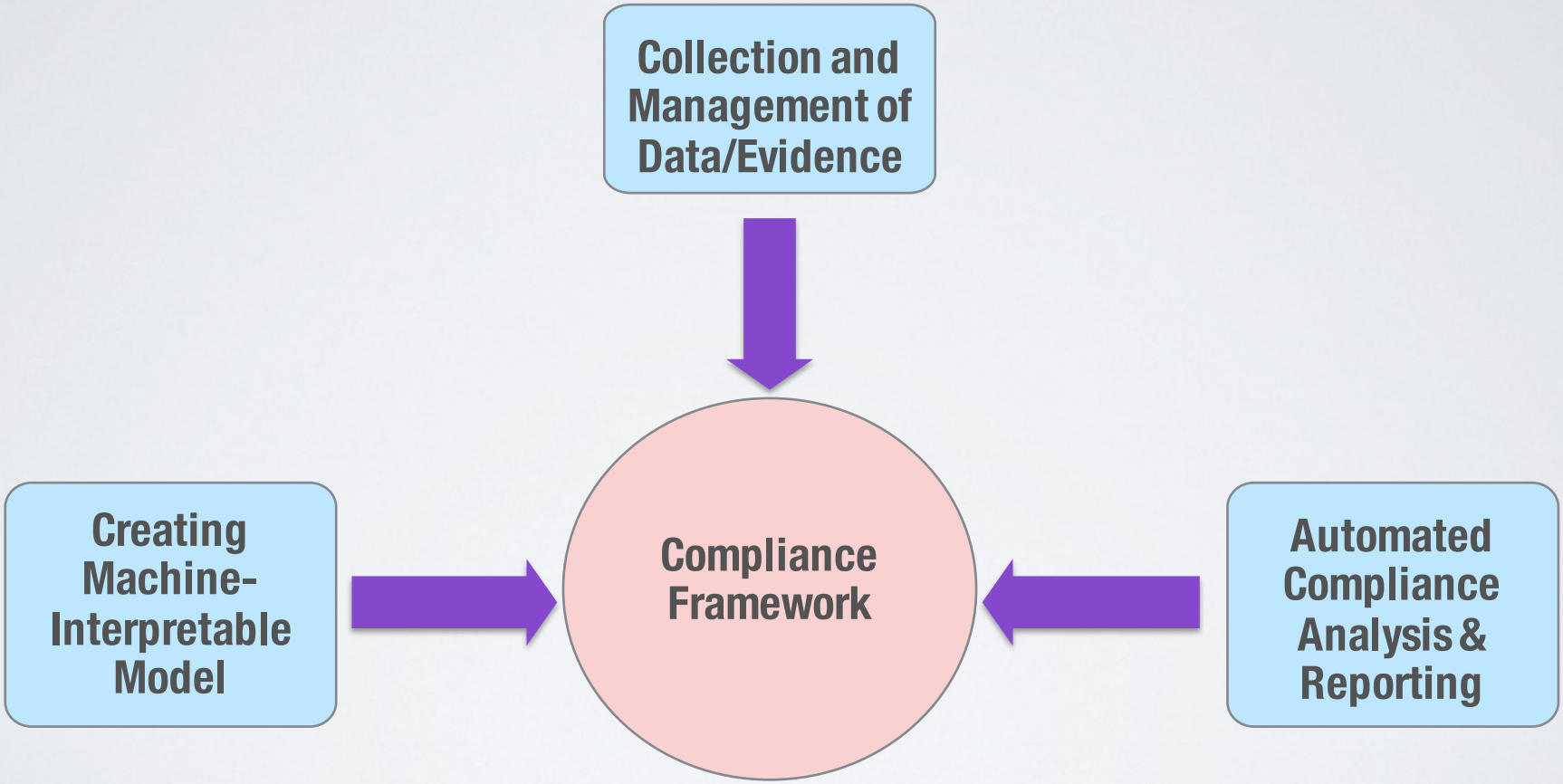
Compliance arguments need to be assessed in a credible manner and based on evidence

What can we do?

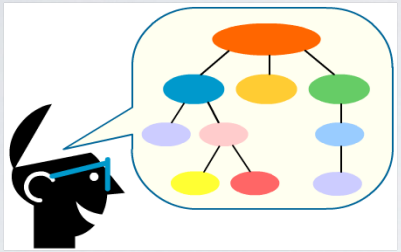
Compliance to Safety Standards

- **Safety-critical systems** have been subject to safety certification for several decades
- **Rigorous compliance assessment** is common practice for safety
- The level of rigor is very likely to extend to data protection and privacy in future years
- Existing work on safety certification can be a **major source of experience and inspiration**

Solution Components



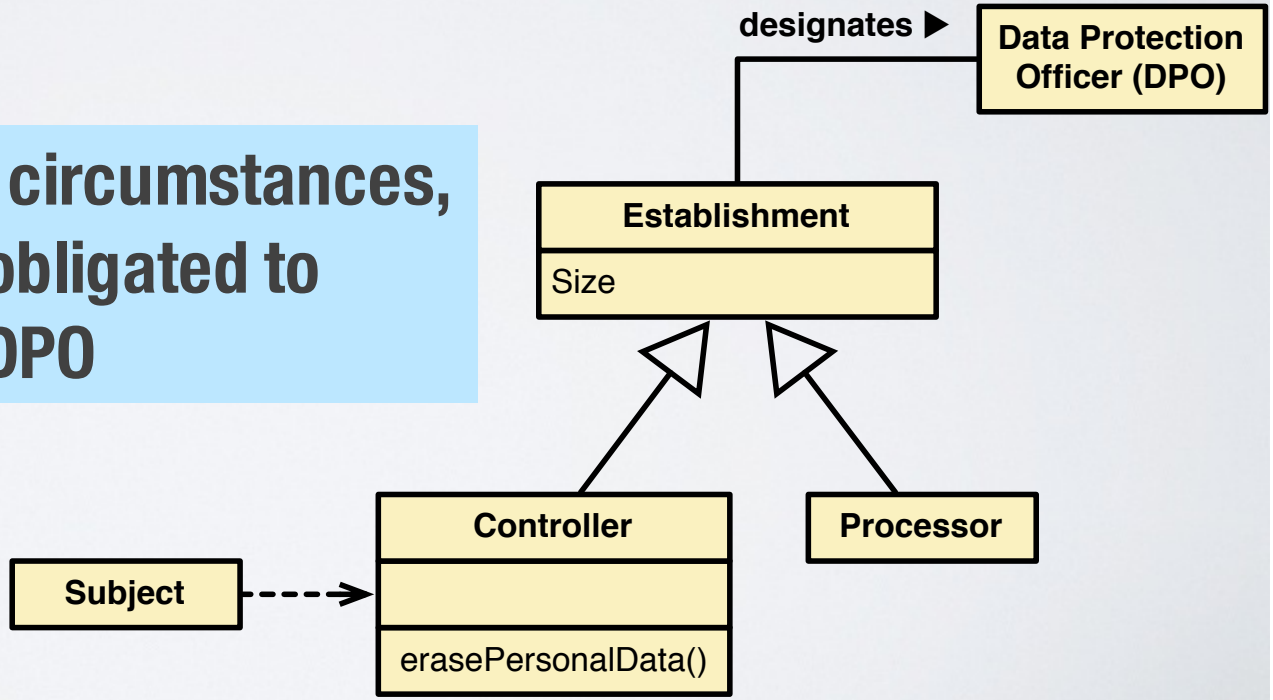
Example Model



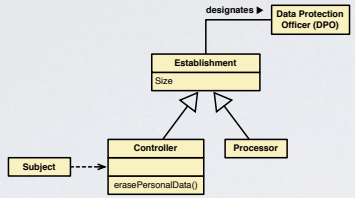
Subject Matter Expert

GDPR Interpretation

Constraint: Under certain circumstances, an establishment is obligated to designate a DPO



Learning from the Safety Critical Domain



Model of the standard or regulation

- Aid to understanding and communication
- Means for collaboration between actors
- Creation of evidence repositories
- Computer-assisted compliance analysis

Evidence Requirements Elaboration

XML

Schema for evidence

basis for

Evidence repository

Compliance Analysis

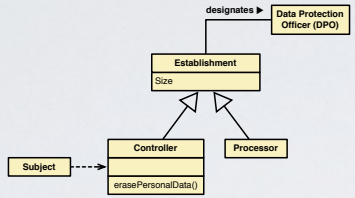
Compliance Results

Specialized checklists, plans, progress measures, agreements, etc.

Assessor

Controller / Processor

Learning from the Safety Critical Domain



Model of the standard or regulation

- Aid to understanding and communication
- Means for collaboration between actors
- Creation of evidence repositories
- Computer-assisted compliance analysis

Evidence Requirements Elaboration

Specialized checklists, plans, progress measures, agreements, etc.

Schema for evidence

basis for

Evidence repository

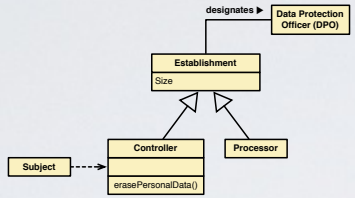
Compliance Analysis

Compliance Results

Assessor

Controller / Processor

Learning from the Safety Critical Domain



Model of the standard or regulation

- Aid to understanding and communication
- Means for collaboration between actors
- Creation of evidence repositories
- Computer-assisted compliance analysis

Evidence Requirements Elaboration

basis for

XML

Schema for evidence

Evidence repository

Specialized checklists, plans, progress measures, agreements, etc.

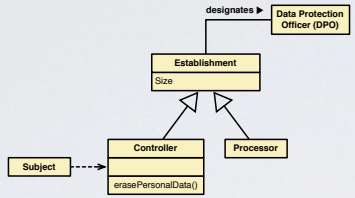
Compliance Analysis

Assessor

Controller / Processor

Compliance Results

Learning from the Safety Critical Domain



Model of the standard or regulation

Aid to understanding and communication

Means for collaboration between actors

Creation of evidence repositories

Computer-assisted compliance analysis

Evidence Requirements Elaboration

XML

Schema for evidence

basis for

Evidence repository

Compliance Analysis

Compliance Results

Specialized checklists, plans, progress measures, agreements, etc.

Assessor

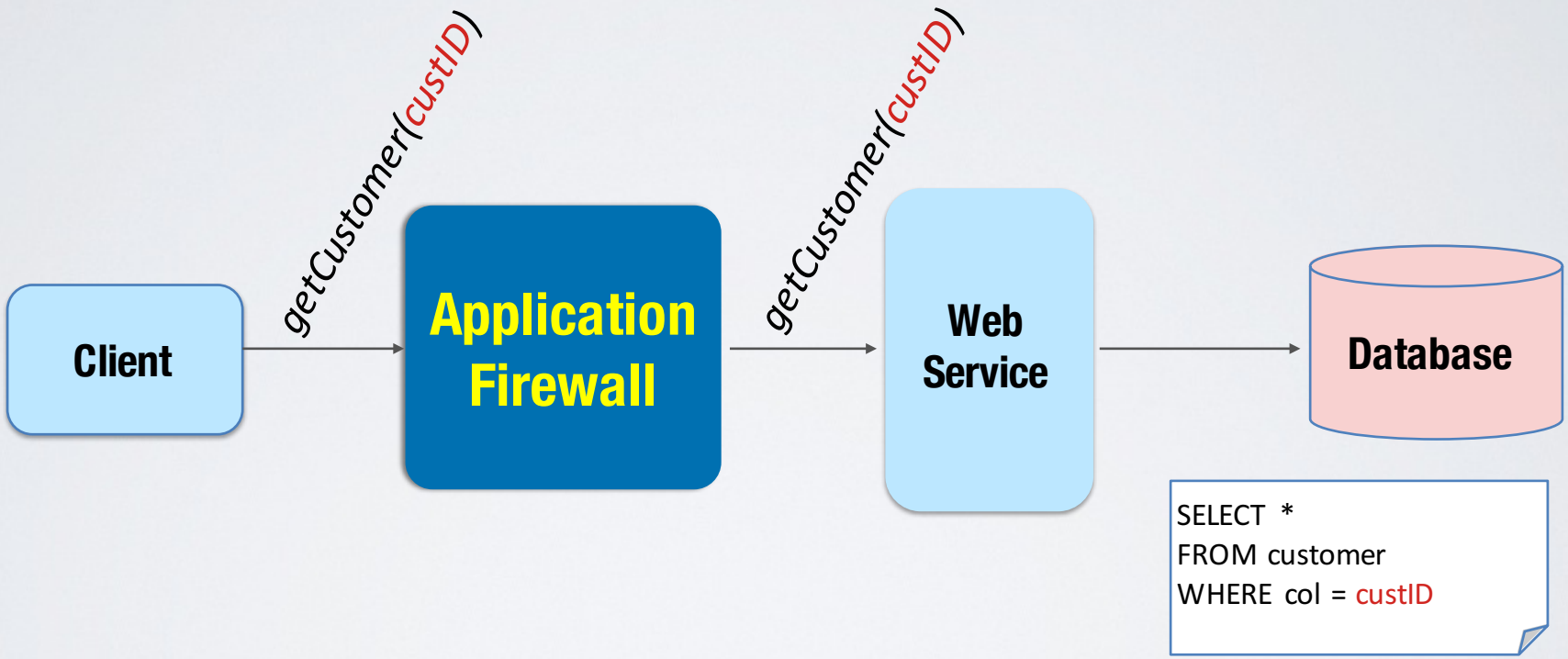
Controller / Processor

Penetration Testing

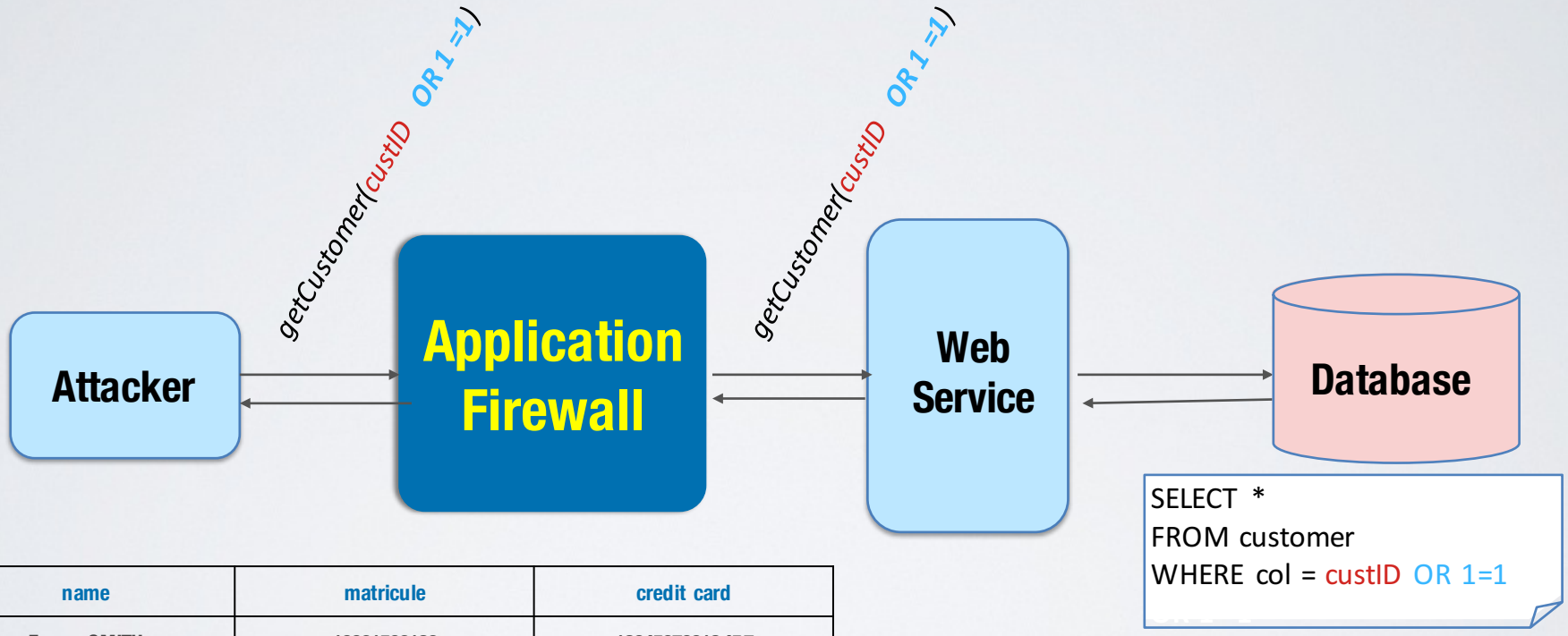
Penetration Testing

- A penetration test is an **attack** on a system to find **vulnerabilities** that an attacker could **exploit**
- The intention is to find security weaknesses, leading to **illegal access to functionality and data.**

Penetration Testing: SQL Injection



Penetration Testing: SQL Injection



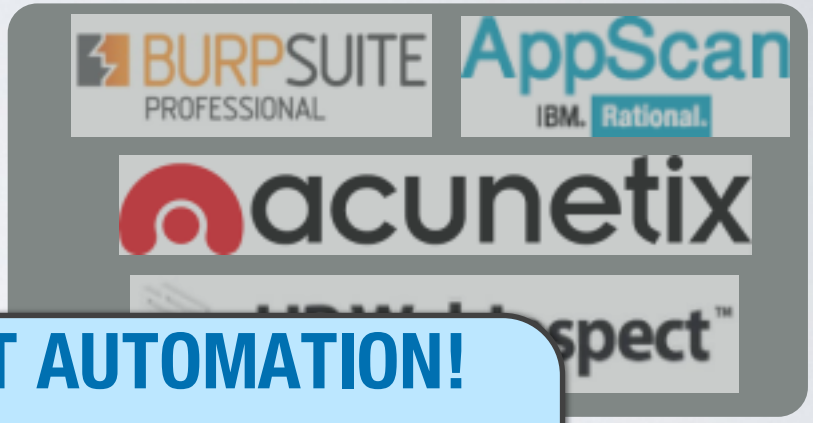
name	matricule	credit card
Emma SMITH	19961506123	12345678912457
Julia BETTEL	19901006321	…..
….	…	….

Data leak!

State of the Practice

Security Con

+



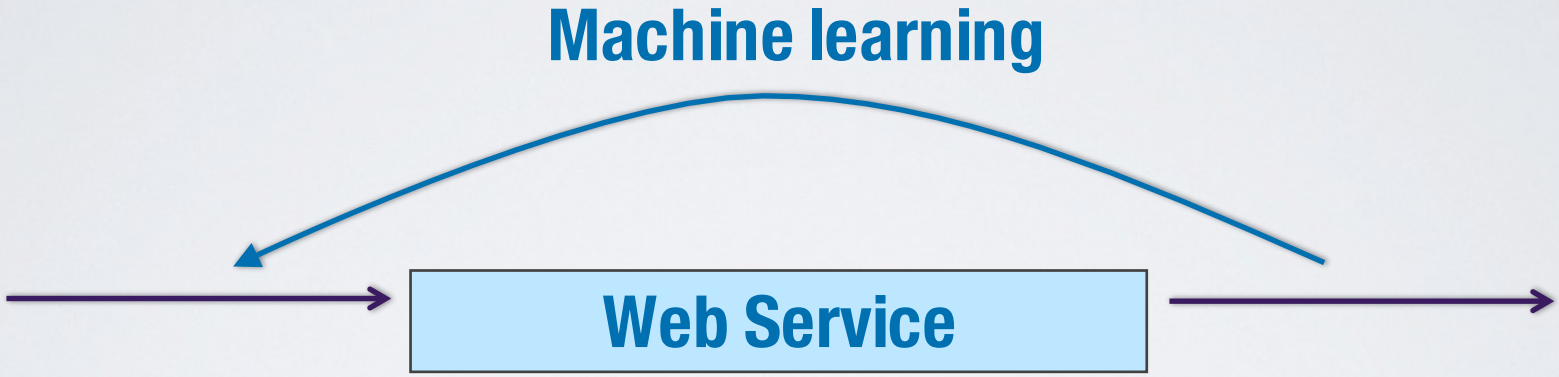
nners

WE NEED BETTER TEST AUTOMATION!

Solution: Automated testing based on machine learning and optimization

- Effort-in
- Effectiveness depends on the competence of the consultants
- Tools: Many false alarms and missed vulnerabilities
- Does not scale

Automated Penetration Testing



- **Attacks:**
  - Inputs
  - XML
  - Access Requests

Maximize chances of finding exploitable vulnerabilities

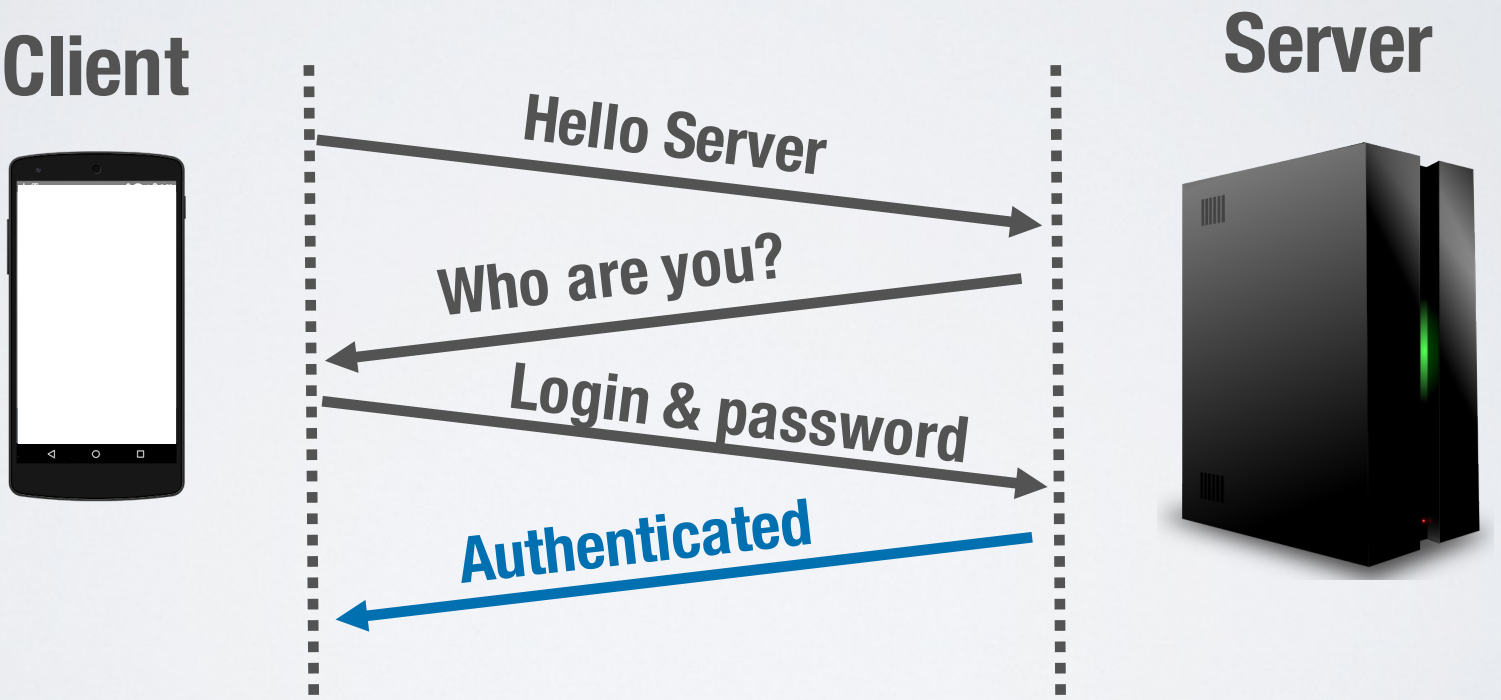
- **Breaches:**
  - Unauthorized access
  - Compromised integrity
  - Denial of Service

Automated Detection of security breaches and data leaks

Protocol Verification

Protocols

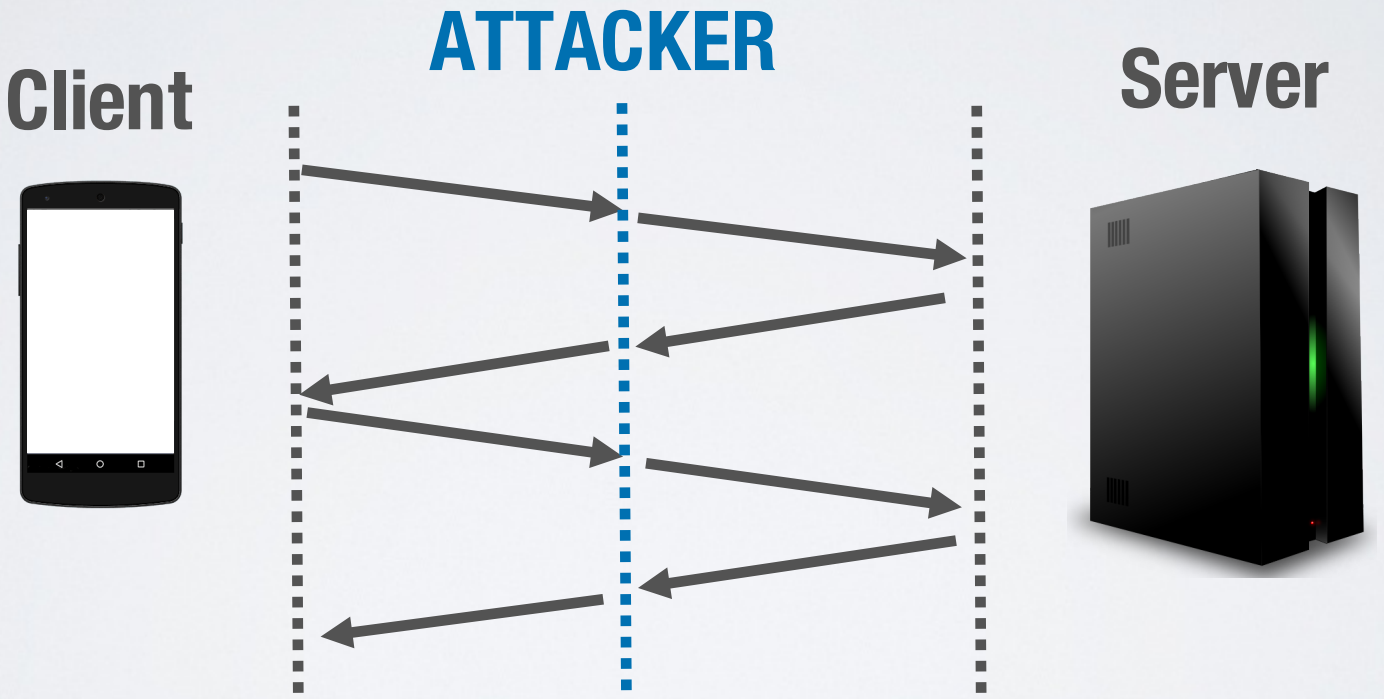
Example: Password Authentication Protocol (PAP)



Security Property: the server authenticates only the right client

Protocols

Example: Password Authentication Protocol (PAP)



Security Property Violation: the server authenticates the attacker

Modeling and Verification

Model

```
specification SequenceDiagram_1_1_option12
channel_model ACM
entity Environment {
  ...
entity Session(…) {
entity C(…) {
  body {
        Actor -Ch_C2SP-> SP : httpRequest(get,ep_uri(SP_authn_C_on_uri:(URI)),nil_req_header,nil_hbody);
        SP -Ch_SP2C-> Actor : httpResponse(code_30x,ep_agent(IdP),?AReq,nil_hbody);
        Actor -Ch_C2IdP-> IdP : httpRequest(get,ep_agent(IdP),AReq ,nil_hbody);
        userlogin;
        IdP -Ch_IdP2C-> Actor : httpResponse(code_200,nil_ep,nil_res_header,htmlForm(?AnySP,?ARsp));
        Actor -Ch_C2SP-> AnySP : httpRequest(post,ep_agent(AnySP),nil_req_header,ARsp);
        AnySP -Ch_SP2C-> Actor : httpResponse(code_200,nil_ep,nil_res_header,?Resource);
              }
}

entity IdP(…) {
    ...
}

entity SP() {
        body
        {
        C -Ch_C2SP-> Actor : httpRequest(get,ep_uri(URI),nil_req_header,nil_hbody);
        ID := fresh();
        Actor -Ch_SP2C-> C : httpResponse(code_30x,ep_agent(IdP),httpBinding(authnRequest(Actor,?IdP,ID),URI),nil_hbody);
        C -Ch_C2SP-> Actor : httpRequest(post,ep_agent(Actor),nil_req_header,postBinding(signedAuthnResponse(invk(pk(IdP)),
        nil_agent, IdP, C, ID), URI));
        Resource := fresh();
        Actor -Ch_SP2C-> C : httpResponse(code_200,nil_ep,nil_res_header,Resource);
        SP_authn_C_on_uri:(URI) := URI;
        }
}
goals
SP_authn_C_on_uri:(_) C *-> SP;
}

body
{
new Session(ch_c2sp_s1, ch_sp2c_s1, ch_idp2c_s1, ch_c2idp_s1, uri, c, sp, idp);
new Session(ch_c2i_s2, ch_i2c_s2, ch_idp2c_s2, ch_c2idp_s2, uri1, c, i, idp);
}
}
```

Model Checker

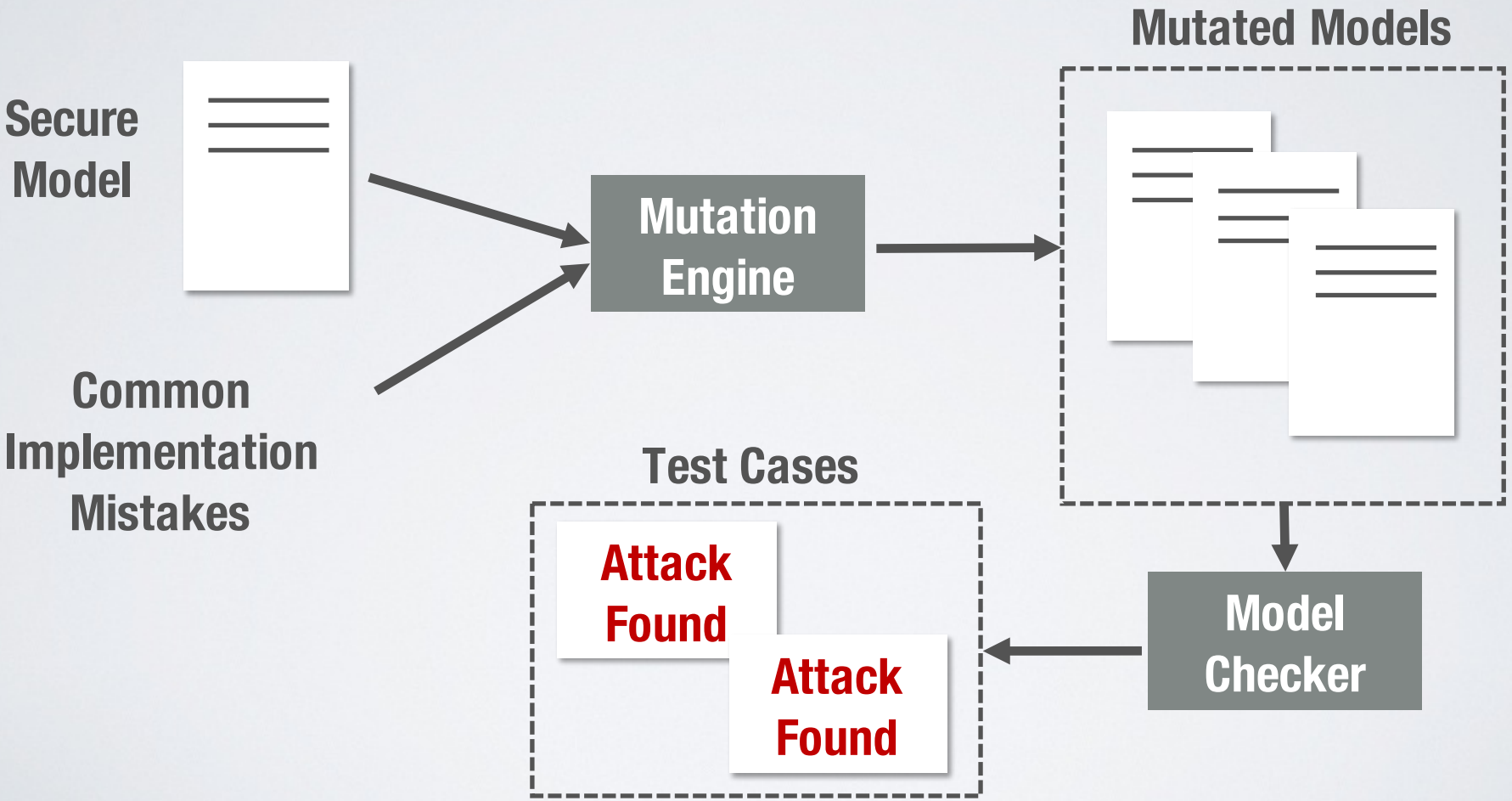
Attack Found

No Attack

HTTP messages and security properties

The model checker is used to identify logical flaws in the protocol design

Testing the Protocol Implementation



Automated Compliance Analysis

Run-time Verification

"A technique that verifies,
after the system is put in operation and is executing, the behavior observed in the system with respect to given properties"

Example property I

Message order and response time: “After every successful completion of a payment, if the payer does not cancel it within 60 seconds, the recipient will receive a confirmation message after at least 70 seconds but not later than 120 seconds”

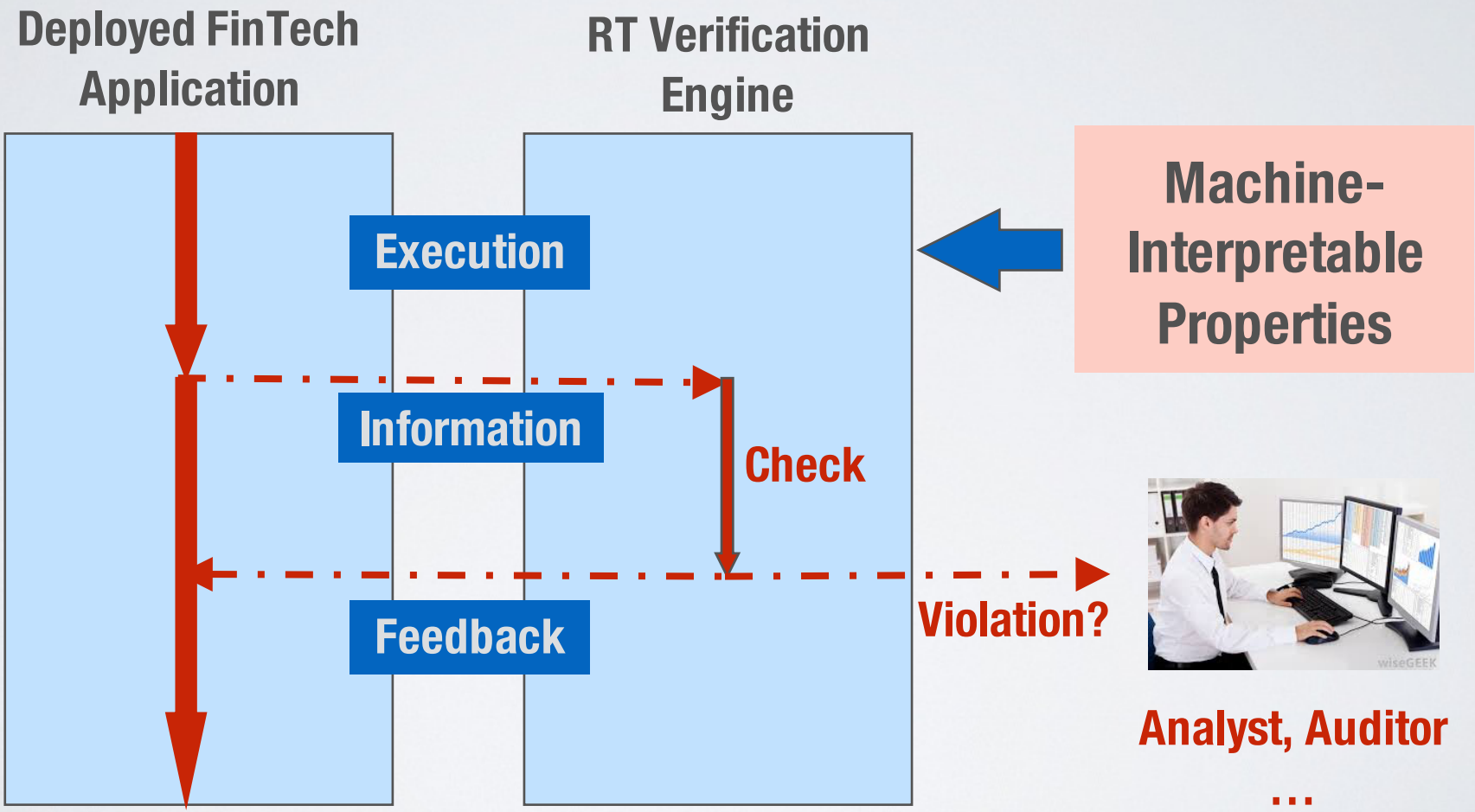
Example property II

- Access control: "An employee with the role 'junior financial analyst' can access the 'Derivatives Trading' application only upon delegation from an employee with role 'specialist financial analyst' and within two hours from the delegation"

Category of Properties

- Regulatory business rules
- Access control and data privacy
- Provisions from standards and best practices
- Service-level agreements

Automation


Deployed FinTech Application
RT Verification Engine
Execution
Information
Check
Feedback
Violation?
Machine-Interpretable Properties
Analyst, Auditor
…

Solutions

$\phi ::= \chi \mid \neg\phi \mid \phi \wedge \phi \mid ((\text{forall} \mid \text{exists})\ \text{id in var}\ ;\ \phi) \mid \textit{Becomes}(\chi) \mid$
$\textit{Until}(\phi, \phi) \mid \textit{Between}(\phi, \phi, K) \mid \textit{Within}(\phi, K) \mid \textit{InFuture}(\phi, K)$

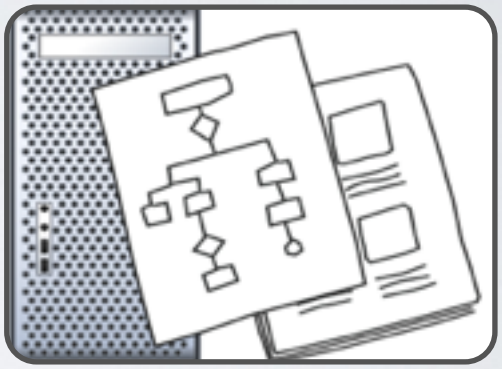
$\chi ::= \psi\ \text{relop}\ \psi \mid \neg\chi \mid \chi \wedge \chi \mid \textit{onEvent}(\mu)$

$\psi ::= \text{var} \mid \psi\ \text{arop}\ \psi \mid \text{const} \mid \textit{past}(\psi, \textit{onEvent}(\mu), n) \mid \textit{count}(\chi, K) \mid$
$\textit{count}(\chi, \textit{onEvent}(\mu), K) \mid \text{fun}(\psi, K) \mid \text{fun}(\psi, \textit{onEvent}(\mu), K) \mid \textit{elapsed}(\textit{onEvent}(\mu))$

$\text{relop} ::= < \mid \leq \mid = \mid \geq \mid >$

$\text{arop} ::= + \mid - \mid \times \mid \div$

$\text{fun} ::= \textit{sum} \mid \textit{avg} \mid \textit{min} \mid \textit{max} \mid \ldots$



Language to express properties

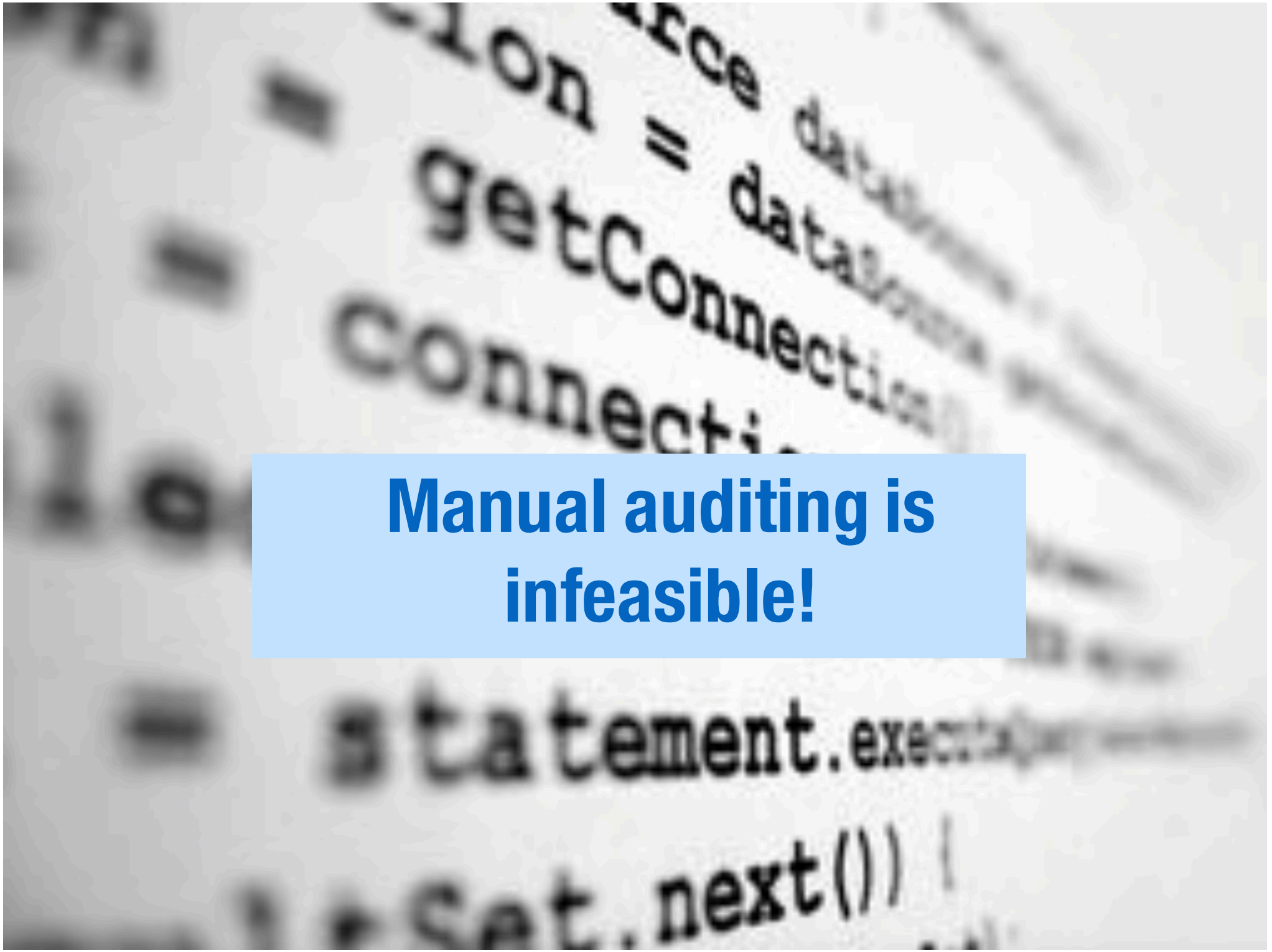
Algorithm to check them based on data

Run-time Architecture to collect data

Security Audits

Security Audits: Definition

Source code analysis to identify, locate, and fix potential security & privacy issues


Manual auditing is infeasible!

Commercial Tools

- Many false alarms
- Miss some vulnerabilities
- Overhead for security audit teams

Vulnerability Verification

Code

Program analysis

Security Slice

Symbolic execution

Condition

Constraint solving

no

yes

Few false alarms

Vulnerability Prediction

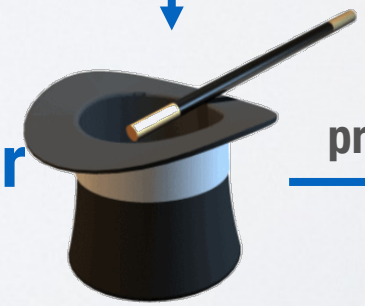
Code

Program analysis

Code characteristics

Machine learning

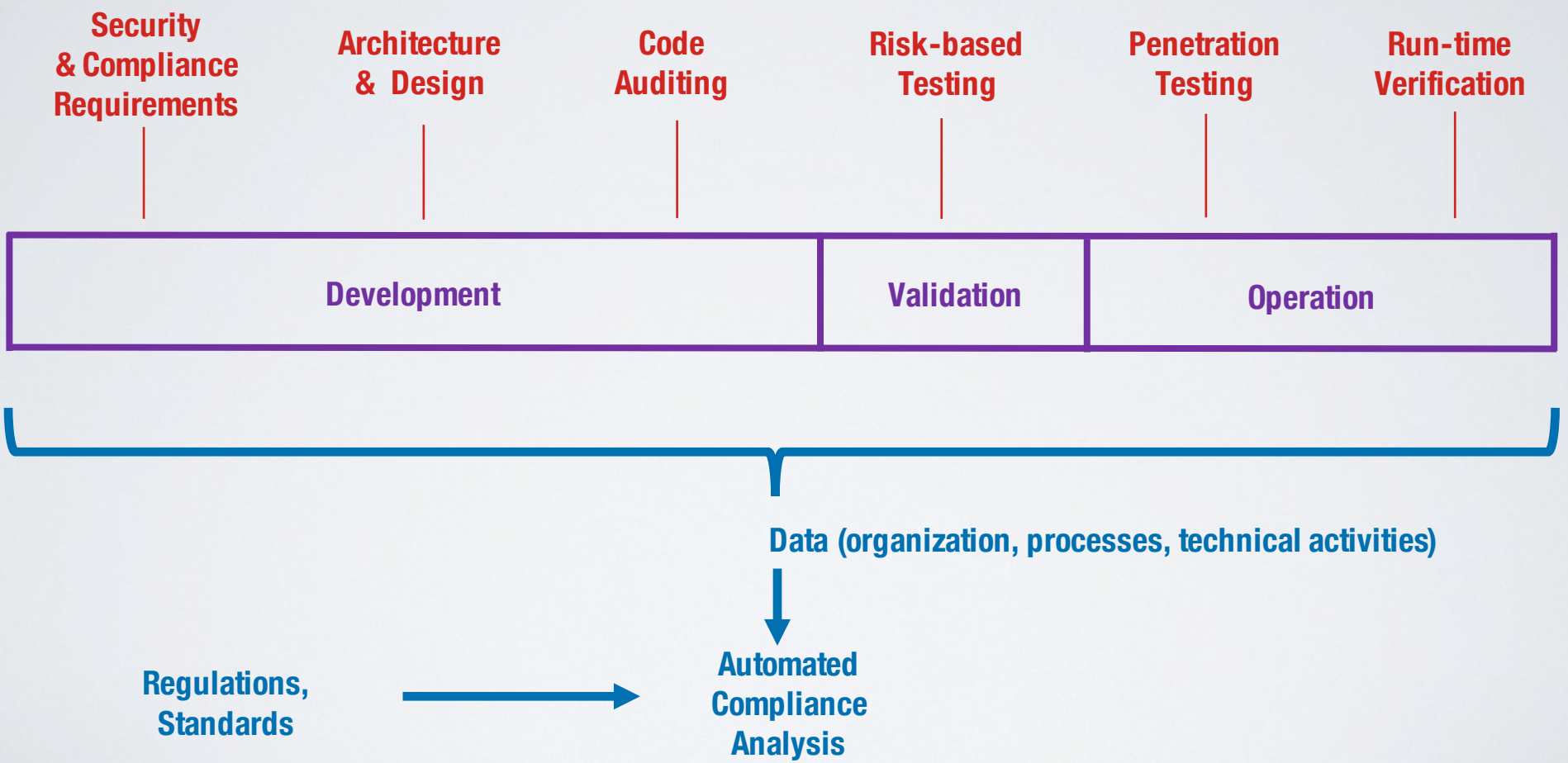
Vulnerability predictor



predicts

How does one get sufficient assurance about security data management and compliance with regulations?

Overall Solution



Additional Contacts

- **Mike Sabetzadeh, Ph.D.:** Regulatory compliance, security requirements
- **Domenico Bianculli, Ph.D.:** Source code auditing, run-time monitoring and verification
- **Annibale Panichella, Ph.D.:** Automated security testing
- **Karl Johannesson:** Project partnerships

SV.lu
software verification & validation

SnT
securityandtrust.lu

Secure and Compliant Data Management in FinTech Applications

Prof. Lionel Briand, FNR PEARL Chair

UL 3X3 FinTech lecture series, February 10th, 2017

uni.lu
UNIVERSITÉ DU LUXEMBOURG