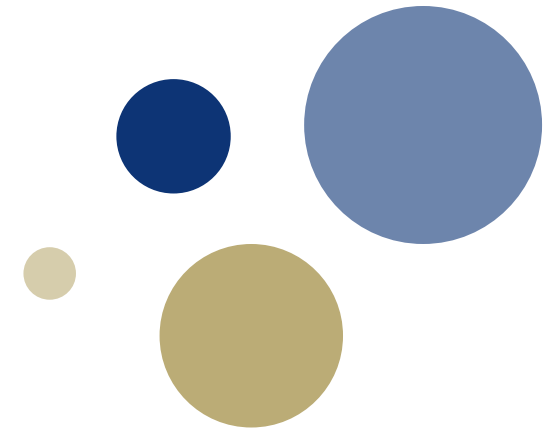




Norwegian University of  
Science and Technology



# Socio-technical constructionism in cyber security

Simon Foley,  
Department of Information Security and  
Communication Technology,  
NTNU Gjøvik

*PreParanoia, Oslo 2019.*





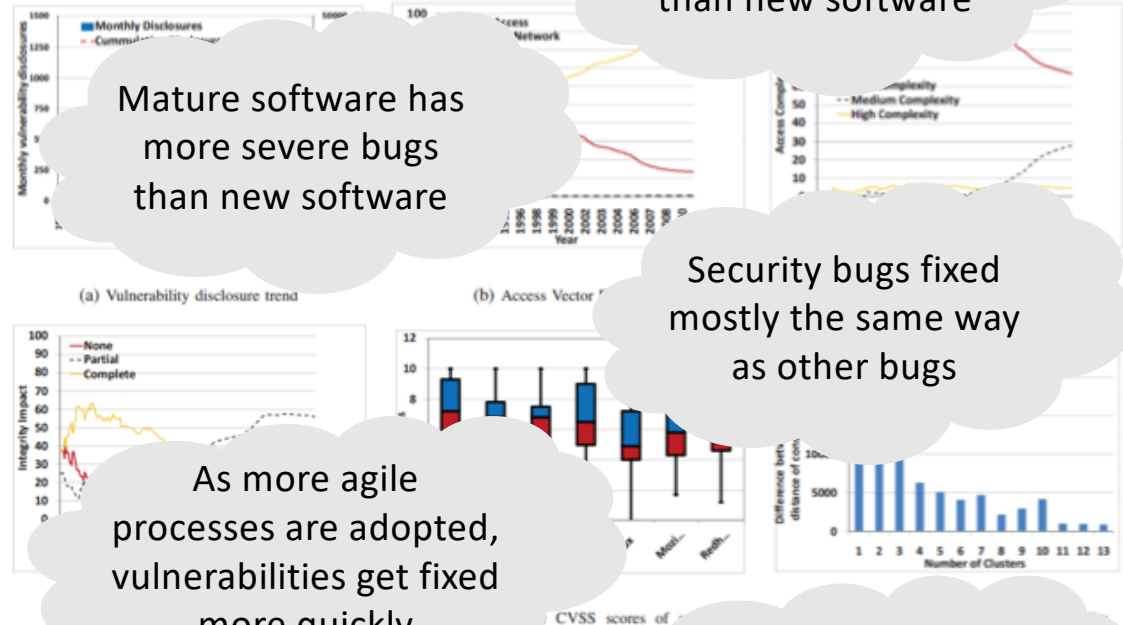
# Quantitative studies

Identify final truths about the world and verify

*“In this paper, we conduct an exploratory measurement study of a large software vulnerability data set containing **46,310 vulnerabilities** disclosed since 1988 till 2011.”*

*“In this paper, we examine how vulnerabilities are handled in large-scale, analyzing **more than 80,000 security advisories** published since 1995. Based on this information, we quantify the performance of the security industry as a whole.”*

*“We analysed **more than 260GB of interdependent project versions** to see how security bugs evolve over time, their persistence, their relation with other bug categories, and their relationship with size in terms of bytecode”*



Mature software has more severe bugs than new software

Mature software has less security bugs than new software

Security bugs fixed mostly the same way as other bugs

As more agile processes are adopted, vulnerabilities get fixed more quickly

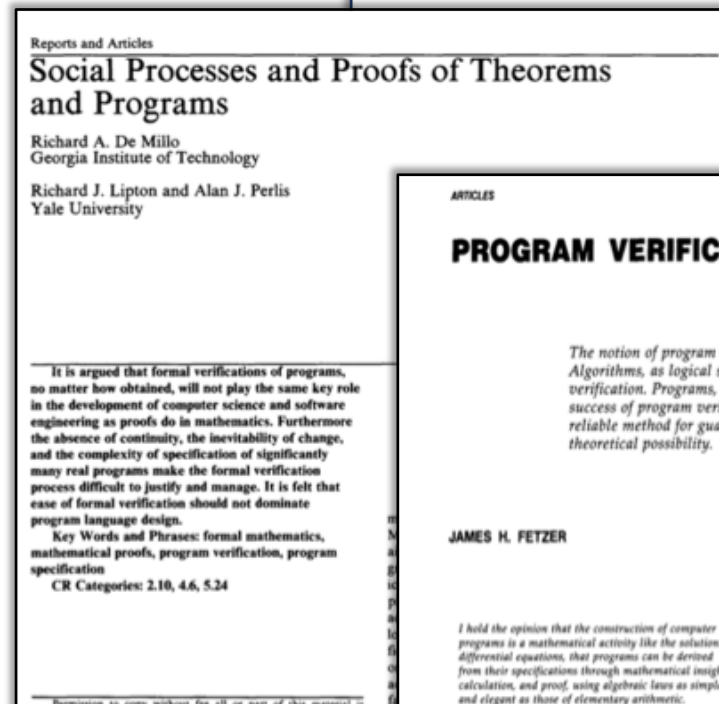
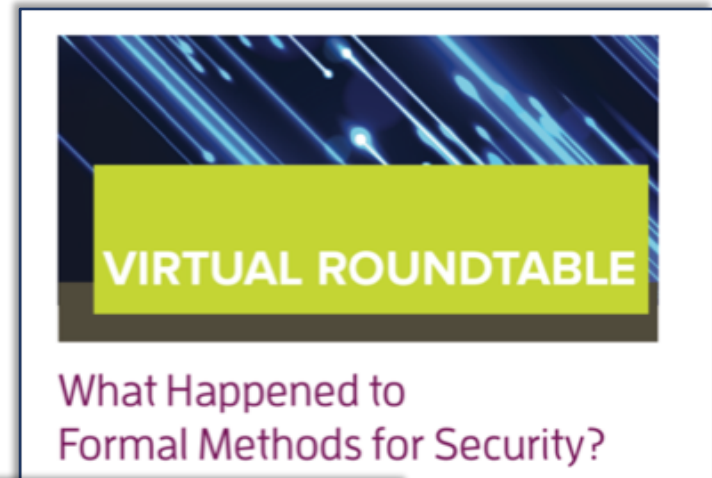
Exploits appear faster than fixes

# What about Formal Methods?

Specify final truths about the system and prove them correct.

*“It has turned out that the world just does not suffer significantly from the kind of problem that our research was originally intended to solve.”*

[CAR Hoare, 1995]



being deployed in regulated industries. If you agree with this claim, it begs two questions: is FM well suited to security concerns, and is assurance primarily the result of compliance and self-governance?

Joseph Williams: FM has indeed been successfully applied to safety-critical systems. One reason is the overwhelming evidence that it results in safer



[ACM 3(9), Sept. 1983]

# World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

Colour YEAR DATA SENSITIVITY Filter

Low High Search...



# Equifax: Struts vulnerability CVE-2017-5638

## CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search  
 View CVE

[Log In](#) [Register](#)

[Home](#)

**Browse :**

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

**Reports :**

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

**Search :**

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

**Top 50 :**

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

**Other :**

- [Microsoft Bulletins](#)
- [Bugtraq Entries](#)
- [CVE Definitions](#)
- [About & Contact](#)
- [Feedback](#)
- [CVE Help](#)
- [FAQ](#)
- [Articles](#)

**External Links :**

- [NVD Website](#)
- [CVE Web Site](#)

### Vulnerability Details : CVE-2017-5638

The Jakarta Multipart parser in Apache Struts 2.3.30-RC1 through 2.3.30-RC2, 2.3.30, 2.3.31, 2.3.32, 2.3.33, 2.3.34, 2.3.35, 2.3.36, 2.3.37, 2.3.38, 2.3.39, and 2.3.40 does not properly handle multipart/form-data requests, allowing remote attackers to execute arbitrary commands via a crafted request. This vulnerability is due to a buffer overflow in the multipart parser. The vulnerability exists because the parser does not properly validate the length of the request body. The vulnerability was discovered by a researcher at Equifax.

Publish Date : 2017-03-10 Last Update Date : 2017-03-10

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Search Twitter](#) [Search YouTube](#) [Search Google](#)

**- CVSS Scores & Vulnerability Types**

CVSS Score	10.0
Confidentiality Impact	Complete (The confidentiality of the system is completely compromised.)
Integrity Impact	Complete (The integrity of the system protection, resulting in the entire system being unusable.)
Availability Impact	Complete (There is a total shutdown of the affected resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances are required to exploit.)
Authentication	Not required (Authentication is not required to exploit.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

**+ Products Affected By CVE-2017-5638**

**+ Number Of Affected Versions By Product**

**+ References For CVE-2017-5638**

ID	Description	Severity	CVSS
CVE-2008-6504	XWork ParameterInterceptors bypass allows OGNL statement execution	Critical	5.0
CVE-2010-1870	XWork ParameterInterceptors bypass allows remote command execution	Critical	5.0
CVE-2011-3923	Parameter remote co		
CVE-2014-0094	Parameter 'class' par manipulat		
CVE-2014-0112	Improves e terceptor tion		

A Complete Guide to the  
Common Vulnerability Scoring System  
Version 2.0

### 2.3.2 Target Distribution (TD)

This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability.

Value	Description
None	No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
Low	Targets exist inside the environment, but on a small scale. Between 1%-25% of the total environment is at risk.
Medium	Targets exist inside the environment, but on a medium scale. Between 26%-75% of the total environment is at risk.
High	Targets exist inside the environment on a considerable scale. Between 76%-100% of the total environment is considered at risk.
Not Defined	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

COMMISSION REGULATION (EC) No 2257/94  
of 16 September 1994  
laying down quality standards for bananas

### III. SIZING

Sizing is determined by:

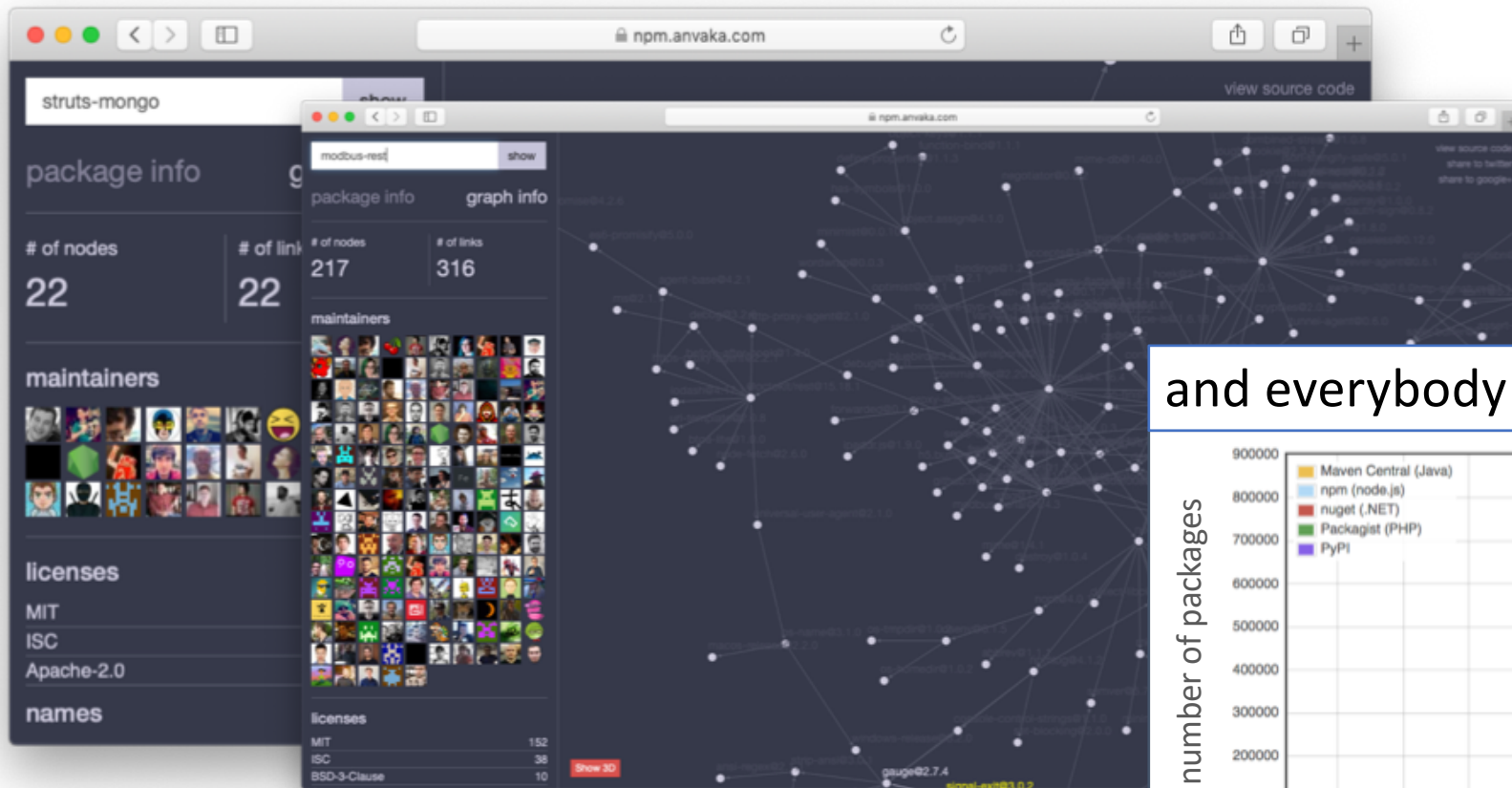
- the length of the fruit expressed in centimetres and measured along the convex face, from the blossom end to the point where the peduncle joins the crown,
- the grade, i.e. the measurement, in millimetres, of the **thickness of a transverse section of the fruit between the lateral faces and the middle, perpendicularly to the longitudinal axis**

The reference fruit for measurement of the length and grade is:

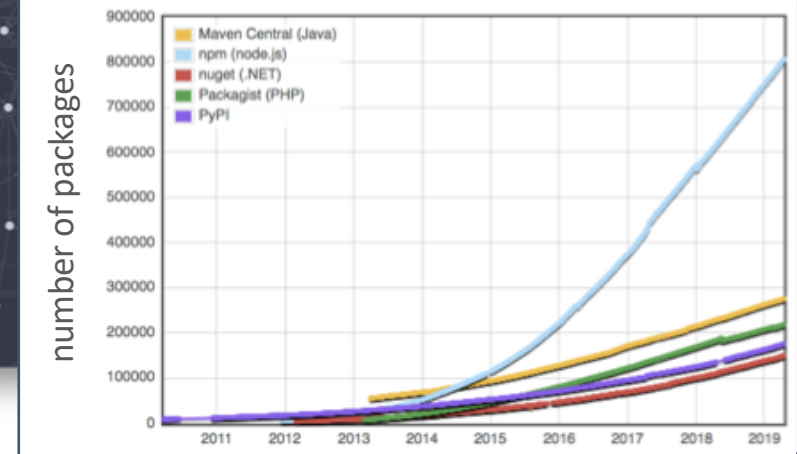
- the median finger on the outer row of the hand,
- the finger next to the cut sectioning the hand, on the outer row of the cluster.

The minimum length permitted is 14 cm and the minimum grade permitted is 27 mm.

# Contemporary systems are convoluted



and everybody is a developer



# And used by people

## The Equifax data breach

### CEO [Smith] testimony:

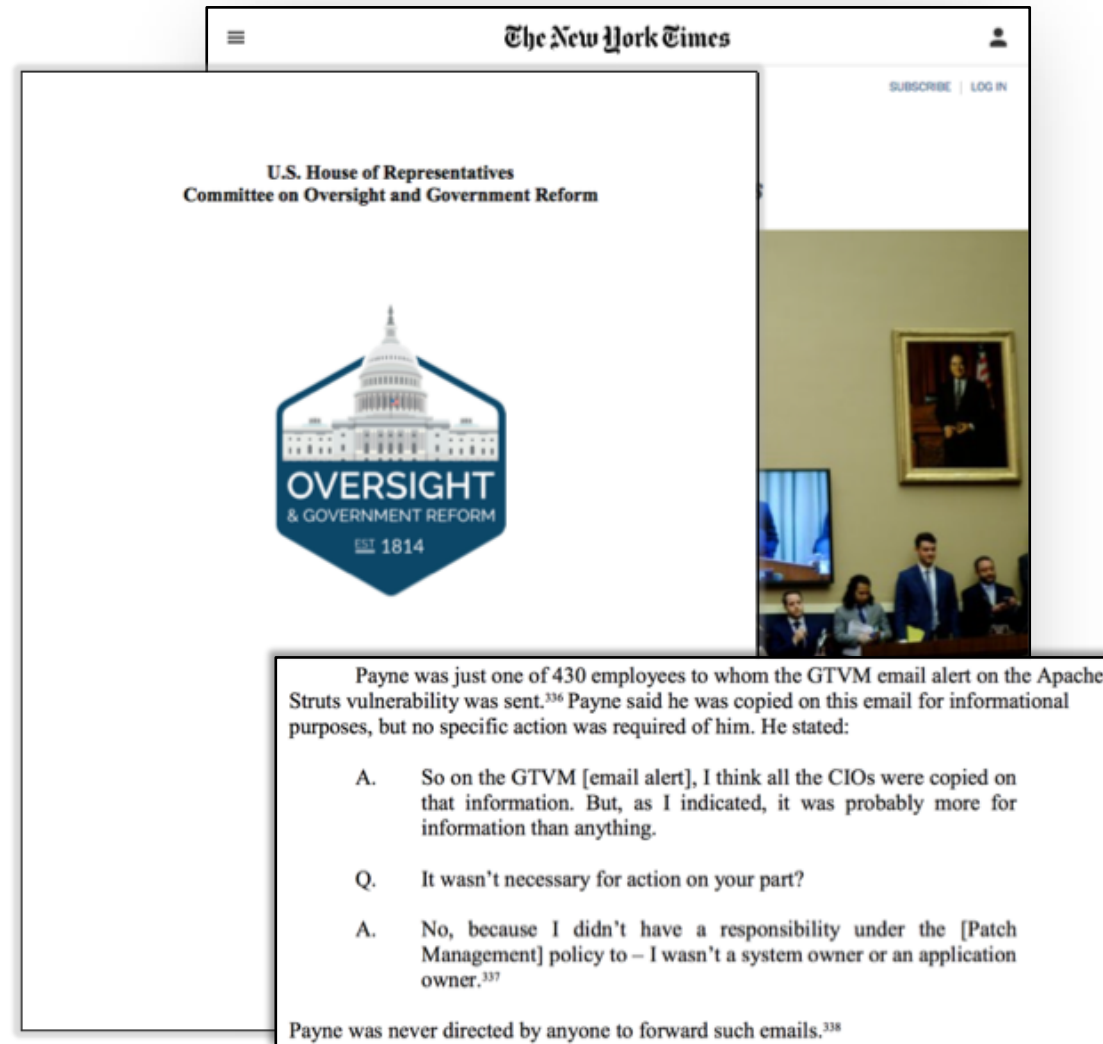
*“The **human error** was that the **individual** who’s responsible for communicating in the organization to apply the patch, did not, ”*

### Individual’s [Payne] response:

*“To assert that a senior vice president in the organization should be forwarding vulnerability alert information to people . . . sort of three or four layers down in the organization on every alert just doesn’t hold water, doesn’t make any sense. **If that’s the process that the company has to rely on, then that’s a problem**”*

## Different people, different realities

- how do we make sense of security?



The New York Times

U.S. House of Representatives  
Committee on Oversight and Government Reform

OVERSIGHT  
& GOVERNMENT REFORM  
EST. 1814

Payne was just one of 430 employees to whom the GTVM email alert on the Apache Struts vulnerability was sent.<sup>336</sup> Payne said he was copied on this email for informational purposes, but no specific action was required of him. He stated:

A. So on the GTVM [email alert], I think all the CIOs were copied on that information. But, as I indicated, it was probably more for information than anything.

Q. It wasn’t necessary for action on your part?

A. No, because I didn’t have a responsibility under the [Patch Management] policy to – I wasn’t a system owner or an application owner.<sup>337</sup>

Payne was never directed by anyone to forward such emails.<sup>338</sup>



# Socio-technical systems as a social construction

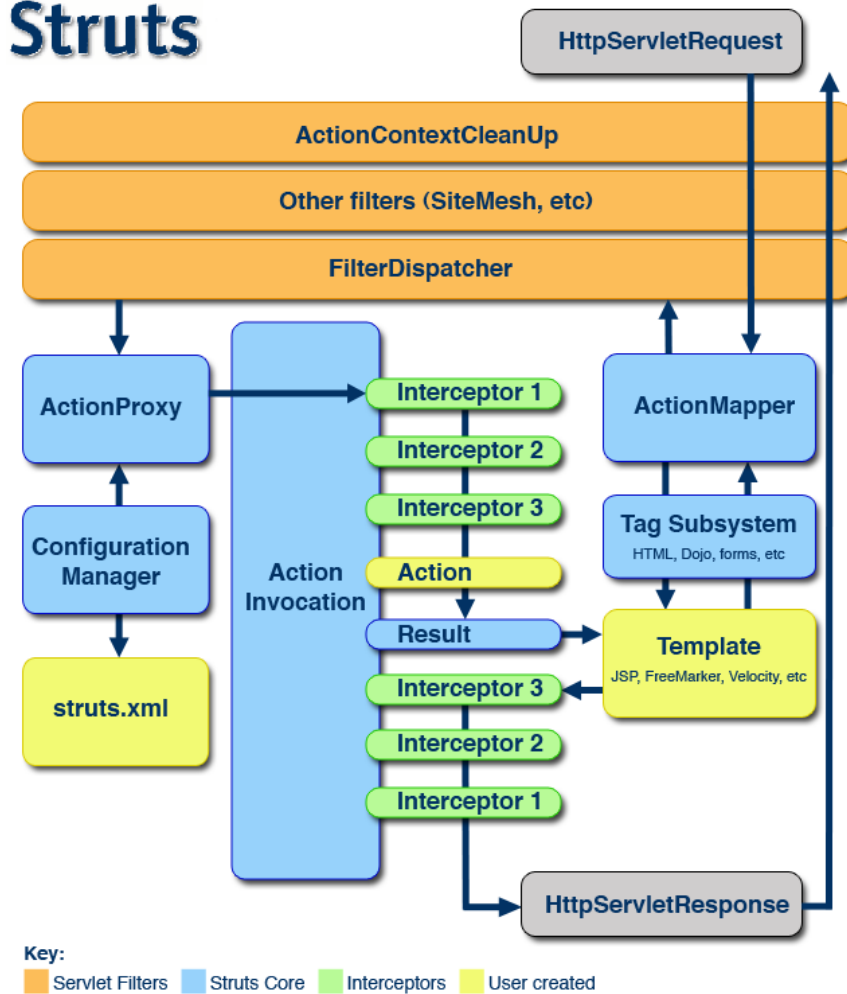
- Systems as the products of humans, deployed and operated by humans.
- Need more than finding final truths and verifying them.
- Qualitative Research techniques
  - Help identify why
  - Discover unknown knowns



# Apache Struts2 MVC web framework

A study of  
parameter interceptor security controls  
(joint work with Olgierd Pieczul)

## Struts



<https://struts.apache.org/>

# Making sense of security vulnerabilities

CVE-2014-0112	
Vendor	Apache
Product	Struts
Release	04/29/2014
Base Score	7.5
Confidentiality	0.275
Integrity	0.275
Availability	0.275
Access Vector	1
Complexity	0.71
Authentication	0.704
Type	CWE-2
Start Version	2.0.0
End Version	2.3.16.1

**Analysis of Recent Struts Vulnerabilities in Parameters and Cookie Interceptors, Their Impact and Exploitation**  
 BY ZUBAIR ASHRAF • MAY 16, 2014  
 Category: Application Security, OWASP, Software & App Vulnerabilities

Whitelisting and blacklisting are not easy to get right. We have seen this recently with the Apache Struts vulnerabilities and multiple back-to-back releases/security announcements 50-005, 50-007 and 50-009; this is something that has been observed in the past as well. I was recently involved in analyzing the 50-009 (Closed) vulnerability.

**: Yet another Struts2 Remote Code**

2012

EC Consult's Struts2 bugs (cool bugs, btw!), I've realized that due to Struts2 still allowed OGNL expression evaluation via parentheses in OGNL expressions stored in action attributes (HTTP parameter values) and the "interceptor" (very similar to CVE-2010-1870).

Interceptors is prohibited since Struts 2.2.3.1 an interceptor of type String to create new Java objects. This can be abused in example to create and name an uninitialized string property can be

Study of 12 years of Struts MVC vulnerabilities

```

    graph LR
      DS[Dark side] --> BS[Blind spots]
      BS --> OF[Opportunistic fix]
      OF --> CIM[Counter-intuitive mechanism]
      RB[Report bias] --> BS
      CI[Compatibility issues] --> OF
      AC[Assumptions about consumers] --> CIM
  
```

with regards to the "By Photo Killing, Problem", Back in of Photo's bug (5/17). A former teacher at Fortify on

Vote for this



# Secure industrial SCADA systems

*"[...] SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks. [...]"*

**CPNI**  
Centre for the Protection  
of National Infrastructure

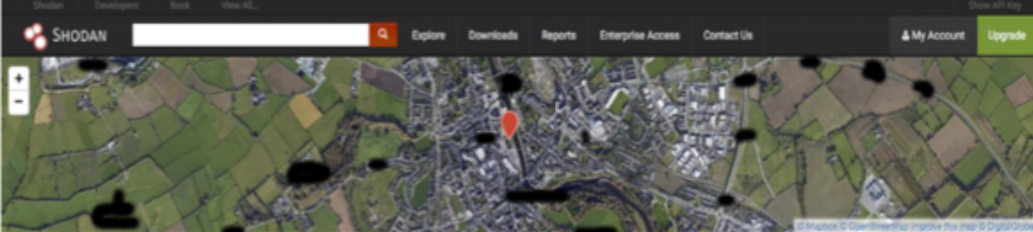
[https://en.wikipedia.org/wiki/File:TASNEE\\_001.jpg](https://en.wikipedia.org/wiki/File:TASNEE_001.jpg)

# An Internet-connected SCADA system

## One year ethnographic study

Shodan located vulnerable Internet connected ICS; operators of system contacted, vulnerability highlighted, remediation/best practices suggested.

Tracked changes over 12 month period.



The screenshot shows a Shodan search result for a system located in Ireland. The system's metadata includes:

City	[REDACTED]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-09-25T12:35:41.830138
Hostnames	84 [REDACTED]
ASN	AS5466

The 'Ports' section shows the following open ports:

102	1723	2080	3389	7547
-----	------	------	------	------

The 'Services' section lists the following services:

102	Basic Hardware: 6ES7 313-2AG18-0AB0 v.8.5
1723	Module: 6ES7 313-2AG18-0AB0 v.8.5
1723	Basic Firmware: v.2.8.12
1723	Firmware: 0
1723	Vendor: Microsoft
3389	Remote Desktop Protocol
3389	Vendor: Microsoft
7547	HTTP/1.1 401 Unauthorized

Red arrows point from the following CVE identifiers to the corresponding services:

- CVE-2015-2177 points to the Basic Hardware service (port 102).
- MS SA 2743314? points to the Basic Firmware service (port 1723).
- CVE-2014-9222? points to the Remote Desktop Protocol service (port 3389).
- CVE-2015-7254? points to the HTTP/1.1 401 Unauthorized service (port 7547).




- Deployed VPN; left SCADA service open
- Security vulnerabilities repeatedly introduced in configuration changes
- Conflict in recommended practices
- Users are trying to get something else done.

# Studying human experience of cyber defense workers

Working in Security Operations Centers & Computer Security Incident Response Teams  
(Joint work with Vivien Rooney)


BEATING  
**BURNOUT**



**SUBSCRIBE**  
from just £1 per issue

**NewStatesman**

CULTURE WORLD SCIENCE & TECH LONG READS NEW TIMES MAGAZINE



**CYBER** 9 MARCH 2016

## Why are SOCs failing?

The fightback against security risks is very real but Luke Jennings, head of research and

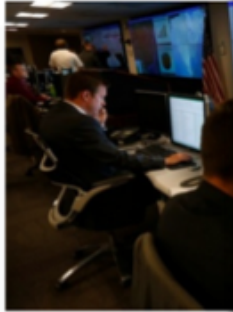
COUNCIL ON FOREIGN RELATIONS

ending Yemen Brexit Refugees North Korea Rohingya

from Net Politics and Digital and Cyberspace Policy Program

## The Challenges Facing Computer Security Incident Response Teams

Blog Post by Guest Blogger for Net Politics  
July 20, 2015




REVIEWS NEWS VIDEO HOW TO SMART HOME CARS GAMES DOWNLOAD

## How Target detected hack but failed to act -- Bloomberg

Despite alerts received through a \$1.6 million malware detection system, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports.

**CSC et HPE Enterprise Services forment désormais DXC Technology.** EN SAVOIR PLUS 

Security



by Lance Whitney  
13 March 2014 2:36 pm GMT  
@lancewhit

QUICK LINKS: State of cybercrime 2016 · Reviews · Video · Newsletters · CSO50 Awards

## CSO


FROM IDG

IN DEPTH

## Avoiding burnout: Ten tips for hackers working incident response

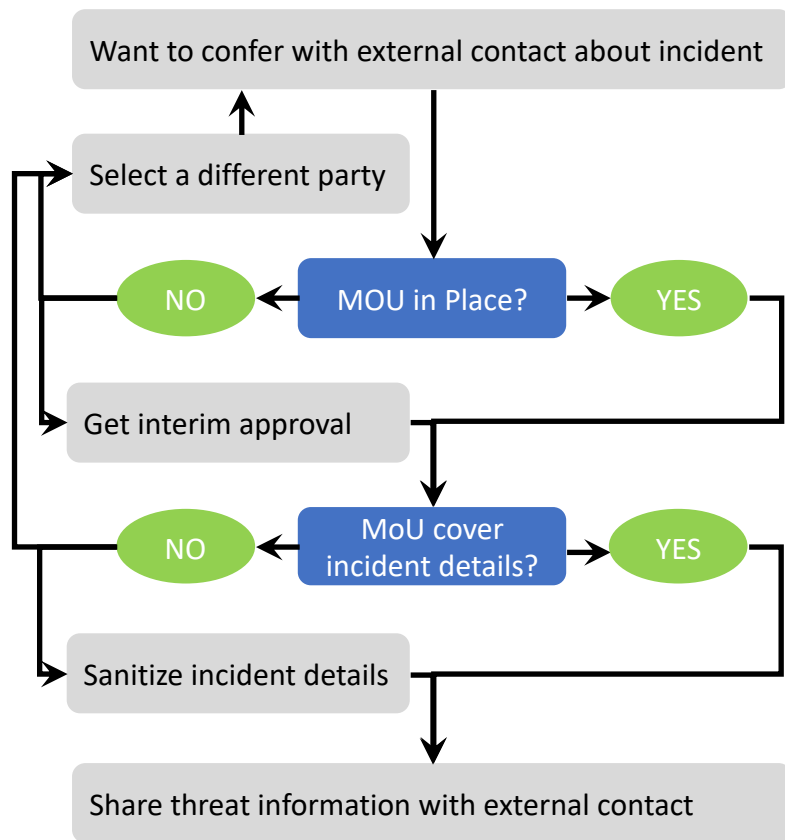
Recent security graduates entering the world of incident response, or those with a strong security background making a career move, face a challenging environment that often leads to frustration and burnout.

By Steve Ragan  
Senior Staff Writer, CSO | APR 30, 2014 8:51 AM PT

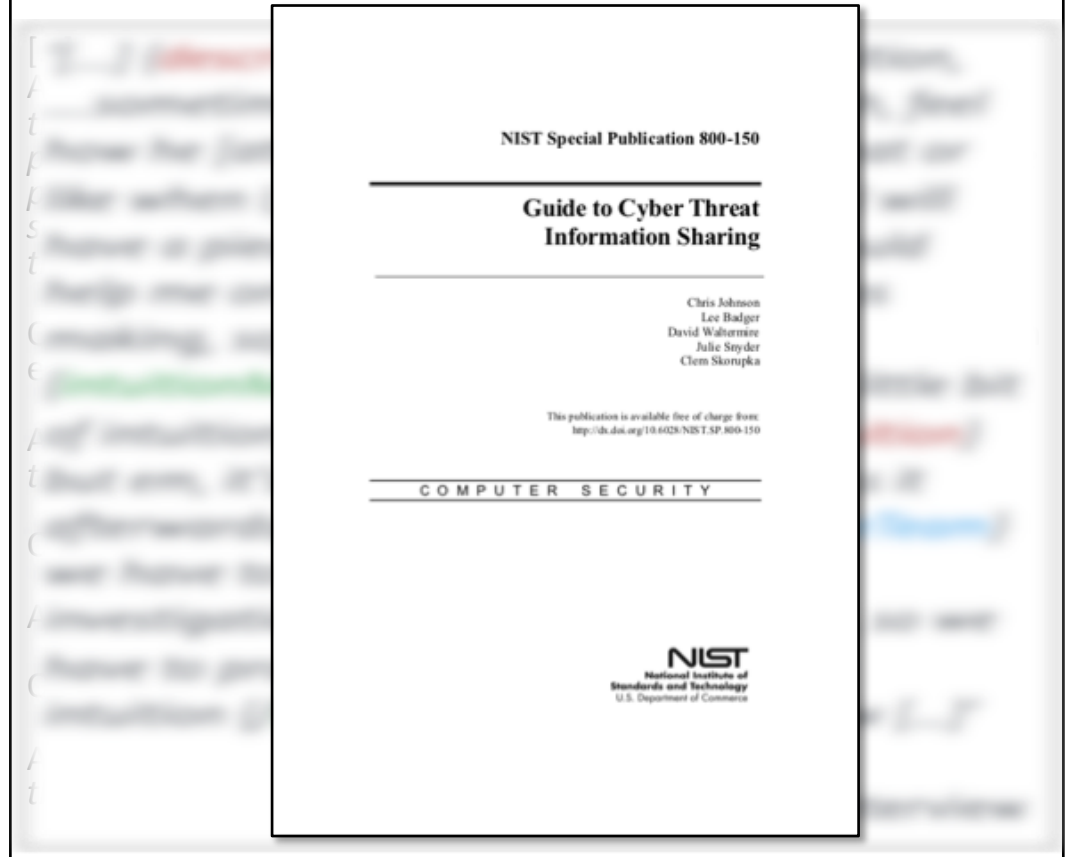


# How people make sense of their world

## Threat information sharing



Extract of semi-structured interview with a person working in computer network defence about threat information sharing:



# Threat Information Sharing

Making sense of experience by constructing multiple identities



## **Team member**

- In a crisis, procedures at a remove to problem-solving activity
- mindful of team when reporting how procedures were followed
- ...

## **Member of the organization**

- Procedures are important
- Procedures help you to work
- Procedures are followed
- ...

## **Member of a global community**

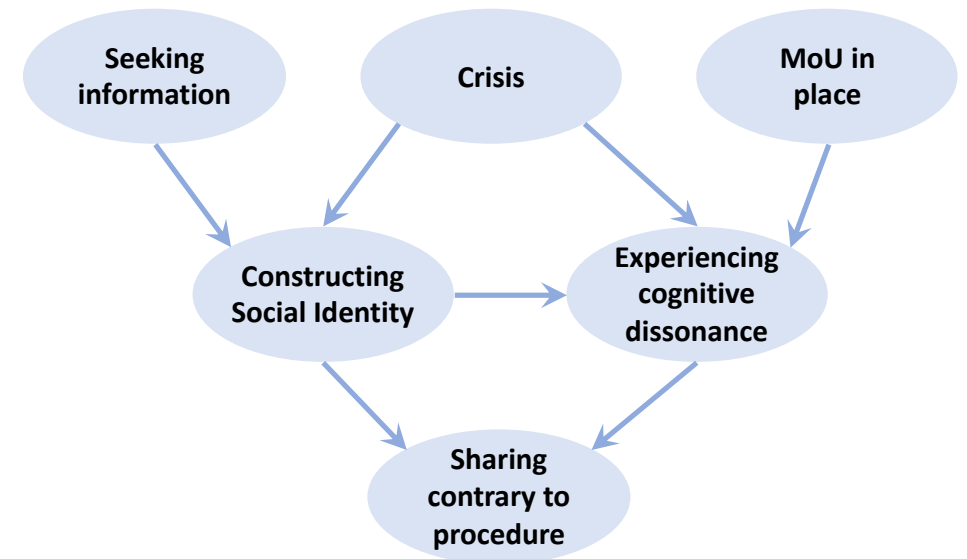
- Sharing information is important.
- Procedures slow you down
- Procedures are sidelined
- ...



# Threat Information Sharing

Procedures as an area of tension

- Social Identity theory: explains how and why identity is created.
- Procedures means different things depending on identity.
- Cognitive Dissonance emerges from multiple realities.
- This is how we understand the experience of Computer Network Defenders.





# HUMAN AFTER ALL

- The “what” and “how” of security
- Need more than finding final truths and verifying them: ask “why”
- Should human transgression be more usefully thought of as a normal part of the security status-quo?