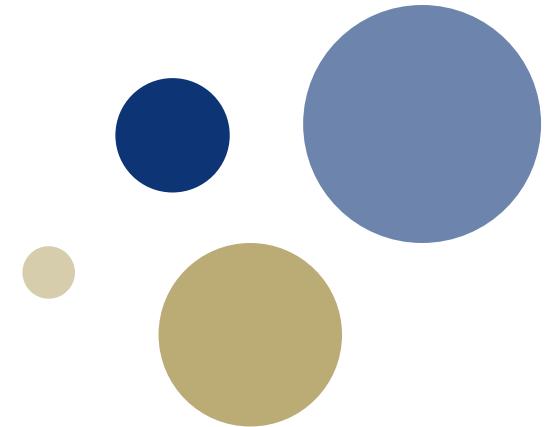




Norwegian University of  
Science and Technology



# Socio-technical constructionism in cyber security

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

*PreParanoia, Oslo 2019.*





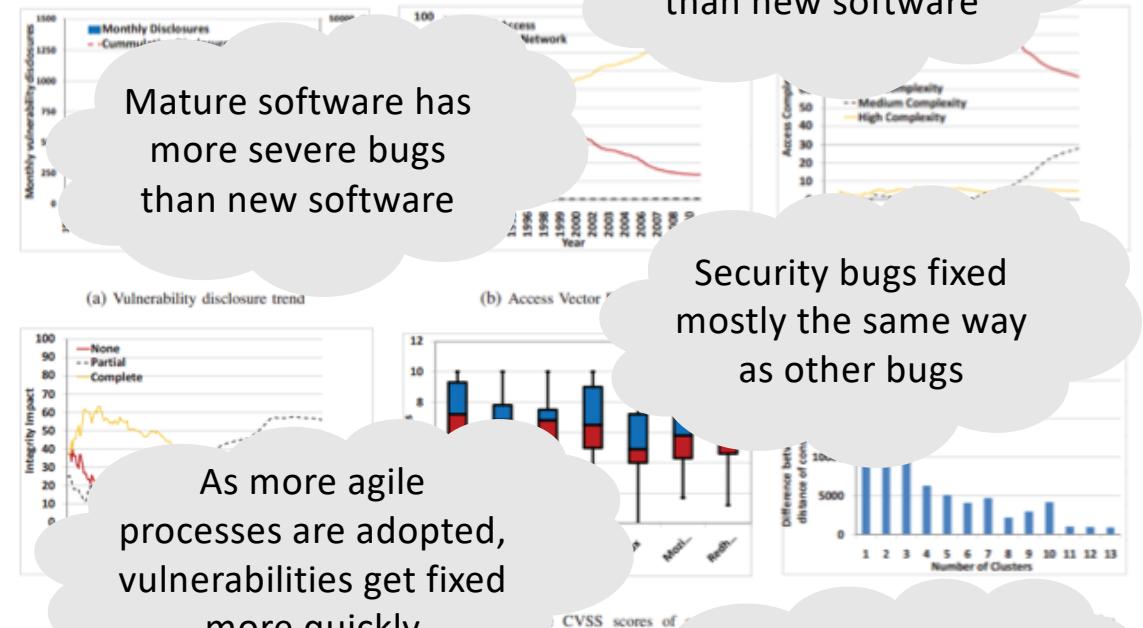
# Quantitative studies

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"*



# 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]



## What Happened to Formal Methods for Security?

Reports and Articles

### Social Processes and Proofs of Theorems and Programs

Richard A. De Millo  
Georgia Institute of Technology

Richard J. Lipton and Alan J. Perlis  
Yale University

It is argued that formal verifications of programs, no matter how obtained, will not play the same key role in the development of computer science and software engineering as proofs do in mathematics. Furthermore the absence of continuity, the inevitability of change, and the complexity of specification of significantly many real programs make the formal verification process difficult to justify and manage. It is felt that ease of formal verification should not dominate program language design.

Key Words and Phrases: formal mathematics, mathematical proofs, program verification, program specification

CR Categories: 2.10, 4.6, 5.24

Permission to copy without fee all or part of this material is

ARTICLES

### PROGRAM VERIFICATION: THE VERY IDEA

The notion of program verification appears to trade upon an equivocation. Algorithms, as logical structures, are appropriate subjects for deductive verification. Programs, as causal models of those structures, are not. The success of program verification as a generally applicable and completely reliable method for guaranteeing program performance is not even a theoretical possibility.

JAMES H. FETZER

I hold the opinion that the construction of computer programs is a mathematical activity like the solution of differential equations, that programs can be derived from their specifications through mathematical insight, calculation, and proof, using algebraic laws as simple and elegant as those of elementary arithmetic.

Their presentation has aroused enormous interest and considerable controversy, ranging from unqualified agreement [expressed, for example, by Glaser [12]; "Such an article makes me delight in being ... a member of the human race!"] to unqualified disagreement [expressed, for example, by Maurer [28]. "The catalog



## 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

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](#)
- [CWE Definitions](#)
- [About & Contact](#)
- [Feedback](#)
- [CVE Help](#)
- [FAQ](#)
- [Articles](#)

**External Links :**

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

**Vulnerability Details : CVE-2017-5638**

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

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	A Complete Guide to the Common Vulnerability Scoring System Version 2.0	
CVE-2014-0094	Parameter 'class' par manipulat	2.3.2 Target Distribution (TD)	
CVE-2014-0112	Improves c terceptor tion	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.	
		<b>Value</b>	<b>Description</b>
		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.

+ Products Affected By CVE-2017-5638  
+ Number Of Affected Versions By Product  
+ References For CVE-2017-5638

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

### III. SIZING

Sizing is determined by:

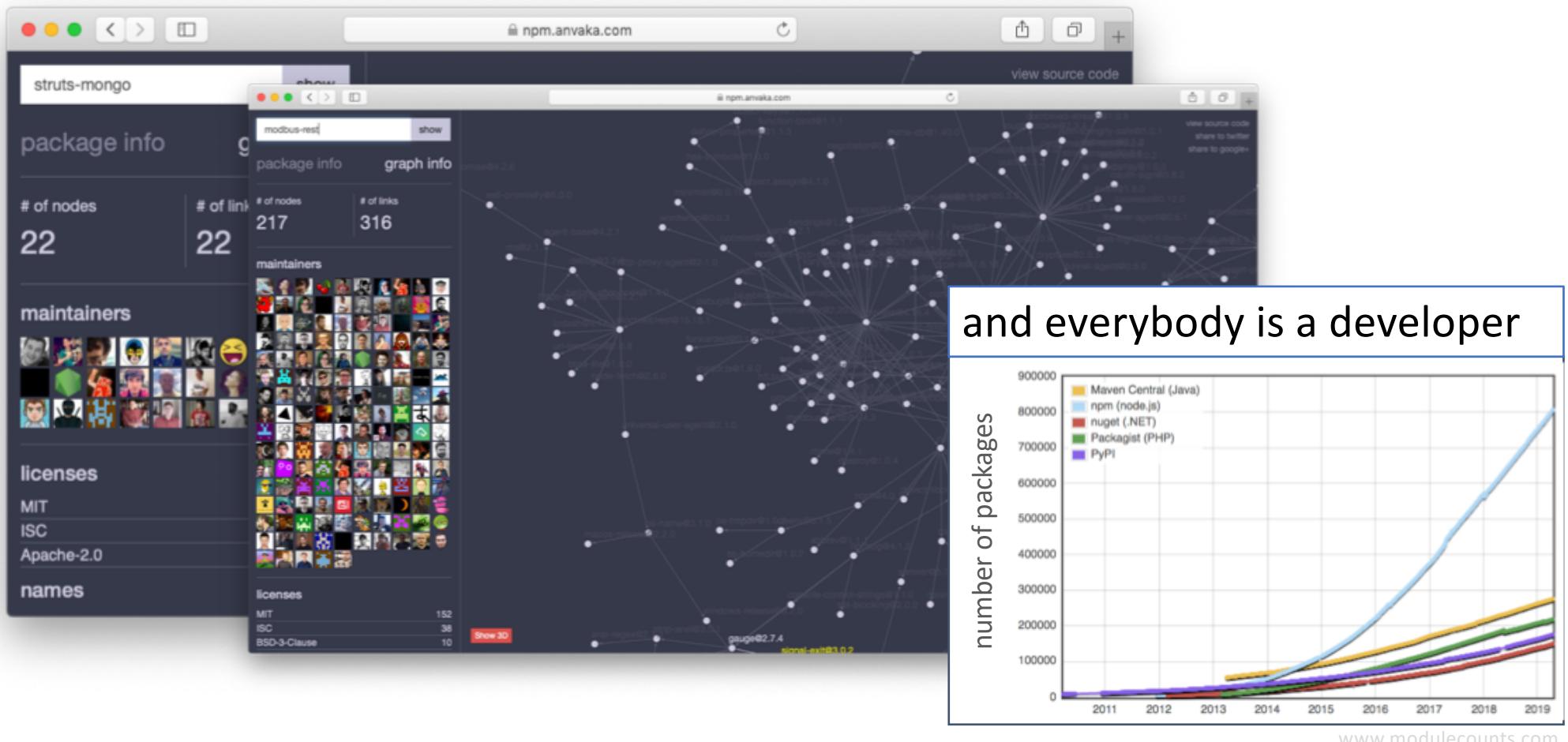
- the length of the fruit expressed in centimetres and measured along the convex face, from the blossom end to the point where the peduncle joins the crown,
- the grade, i.e. the measurement, in millimetres, of the thickness of a transverse section of the fruit between the lateral faces and the middle, 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 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 screenshot shows a news article from The New York Times. At the top right is the The New York Times logo and a user icon. Below it is a navigation bar with 'SUBSCRIBE' and 'LOG IN'. The main content area features the logo of the U.S. House of Representatives Committee on Oversight and Government Reform, which is a blue hexagon containing a white silhouette of the U.S. Capitol building and the words 'OVERSIGHT & GOVERNMENT REFORM EST 1814'. To the right of the logo is a photograph of a hearing room with several people seated at a table. The text of the article discusses Payne being one of 430 employees copied on an email about a Apache Struts vulnerability, and his responses to questions about the process.

**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

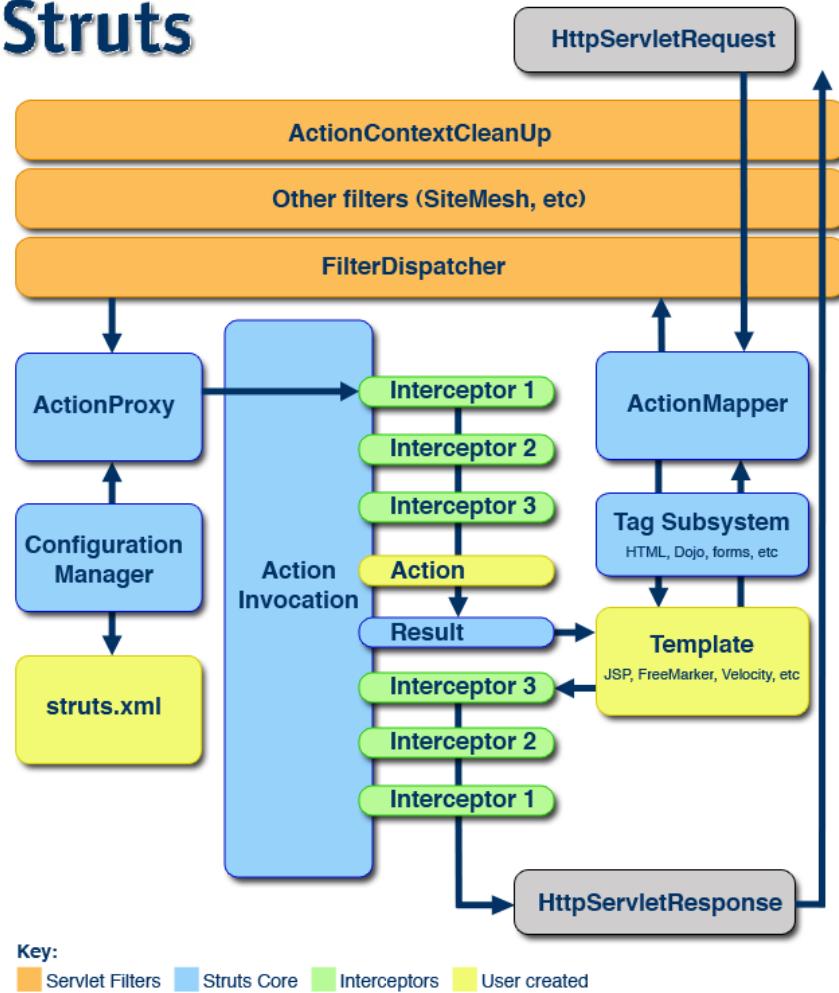
- Systems as the products of humans, deployed and operated by humans.
- Need more than finding final truths and verifying them.
- Qualitative Research techniques
  - Help identify why
  - Discover unknown knowns



# Apache Struts2 MVC web framework

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

## Struts

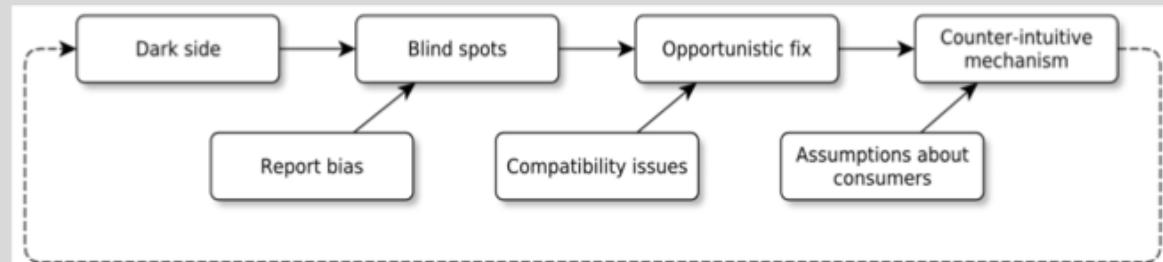


<https://struts.apache.org/>

# 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-284
Start Version	2.0.0
End Version	2.3.16.1

## Study of 12 years of Struts MVC vulnerabilities



... probably I have not been clear with what I meant.  
The problem is not in the session values itself, but how they are evaluated.

Hiato Killing  
Votes:  
@Vota for this issue  
the first time you visit  
the site  
the file "cross-consult.txt"  
contains the line "HiatoKilling"  
use it in these examples is of no importance

### Analysis of Recent Struts Vulnerabilities in Parameters and Cookie Interceptors, Their Impact and Exploitation

BY ZUBAIR ASHRAF • MAY 16, 2014

Categories: Application Security, IBM X-Force, 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 [SS-002](#), [SS-001](#) and [SS-003](#). This is something that has been observed in the [Java](#) as well. I was recently involved in analyzing the [SS-001](#) Client code and I am providing guidance to our customer about

Comments on Aug 5, 2012  
HHW-3600 300  
spikes committed on Aug 5, 2012

Comments on Jul 20, 2012  
HHW-3643 adds proper extensible  
commit comment on Jul 20, 2012

Comments on Feb 22, 2012  
HHW-3648 changes access  
comment on Feb 22, 2012

, 2012  
: Yet another Struts2 Remote Code

EC Consult's Struts2 bugs (cool bugs, btw!), I've realized that due to Struts2 still allowed OGNL expression evaluation via parentheses I can expressions stored in action attributes (HTTP parameter values) leading to arbitrary code execution in Struts2 applications with default interceptor), very similar to CVE-2010-1870.

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

make into account the  
String) rather than

with regards to the  
by Hiato Killing.  
Problem: Back In  
of Hiato's bug  
2012. A former  
archer at Fortify an  
interface and also

5

# Secure industrial SCADA systems

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



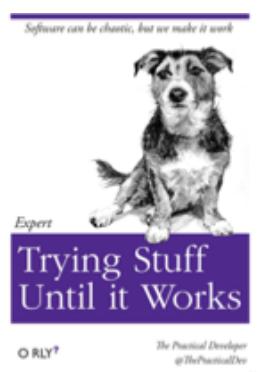
[https://en.wikipedia.org/wiki/File:TASNEE\\_001.jpg](https://en.wikipedia.org/wiki/File:TASNEE_001.jpg)

# An Internet-connected SCADA system

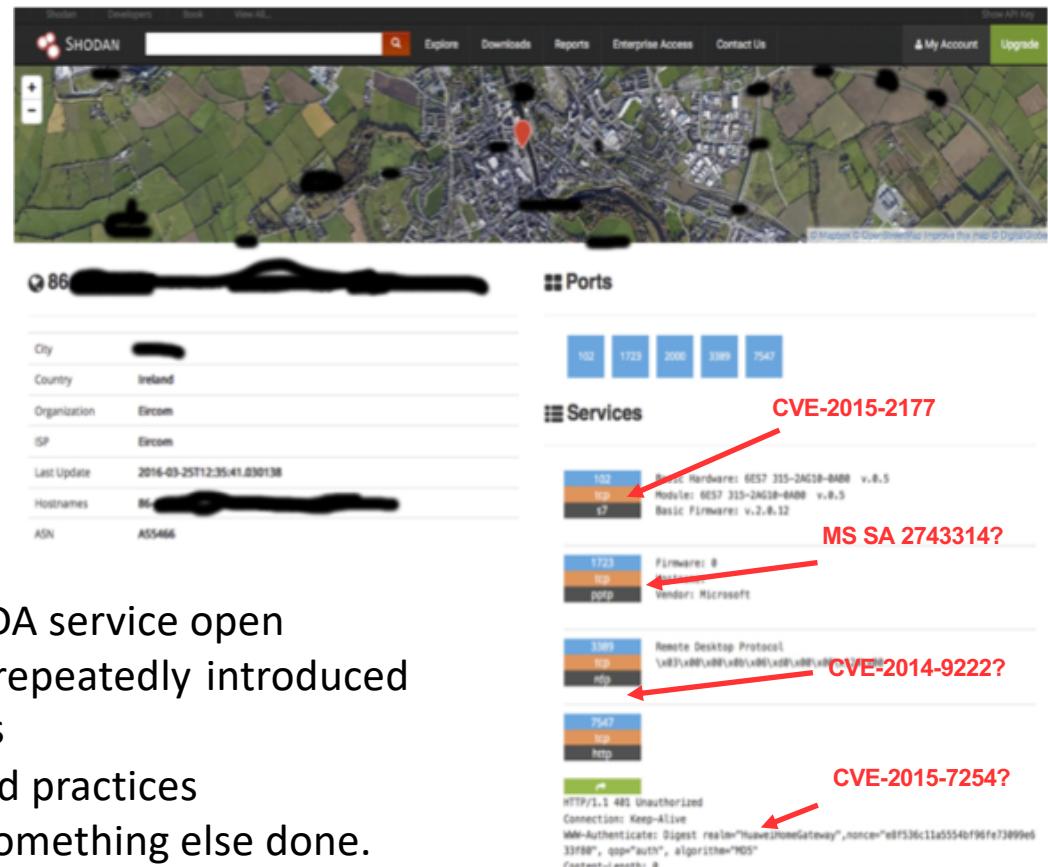
## One year ethnographic study

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

Tracked changes over 12 month period.



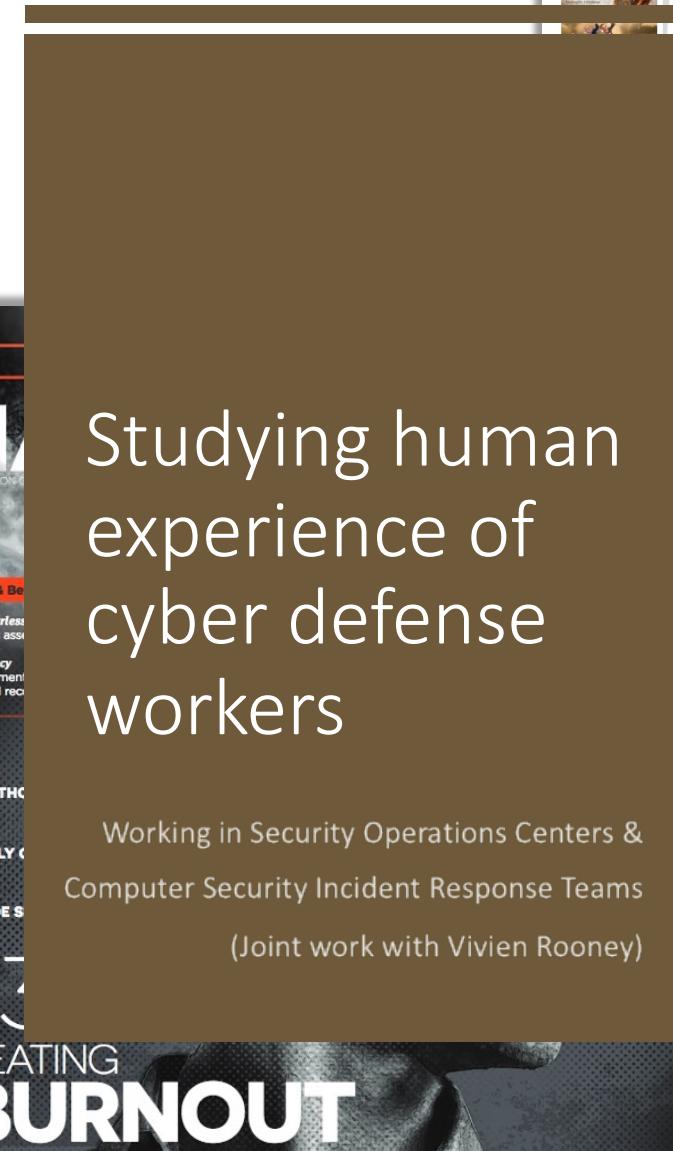
- Deployed VPN; left SCADA service open
- Security vulnerabilities repeatedly introduced in configuration changes
- Conflict in recommended practices
- Users are trying to get something else done.



# Studying human experience of cyber defense workers

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

BEATING  
**BURNOUT**



**NewStatesman**

**SUBSCRIBE**  
from just £1 per issue

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

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



SEARCH

## 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 ► DXC.DXC.technology

Security



by Lance Whitney  
13 March 2014 3:36 pm (EST)  
@lancewhit1 #



QUICK LINKS: State of cybercrime 2018 • Reviews • Video • Newsletters • CSO50 Awards •  
INSIDER Sign In

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 strong security background making a career move, face a challenging environment that often leads to frustration and burnout.

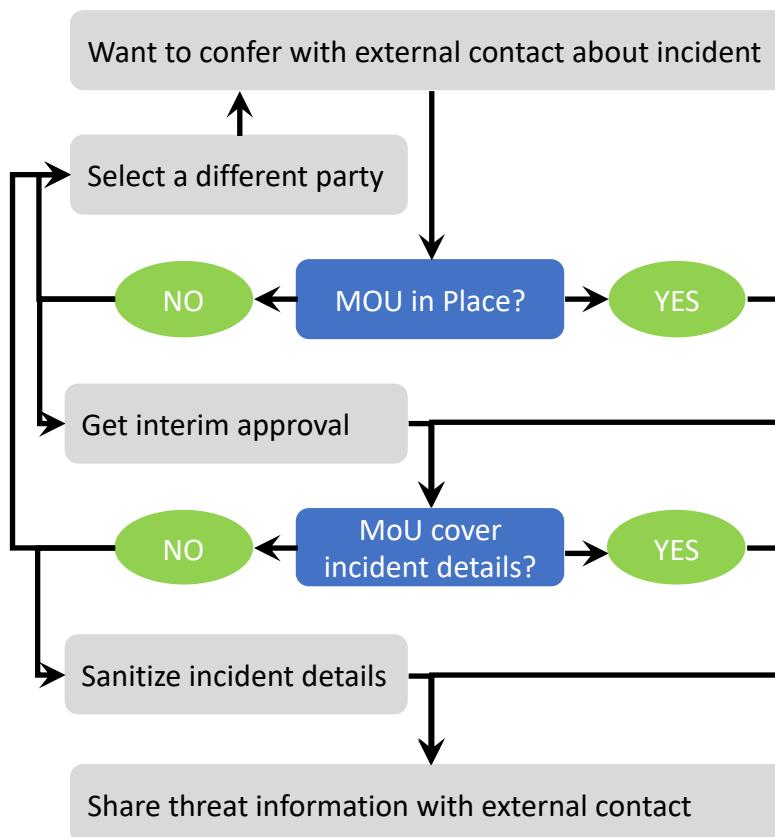


By Steve Ragan  
Senior Staff Writer, CSO | APR 30, 2014 8:51 AM PT

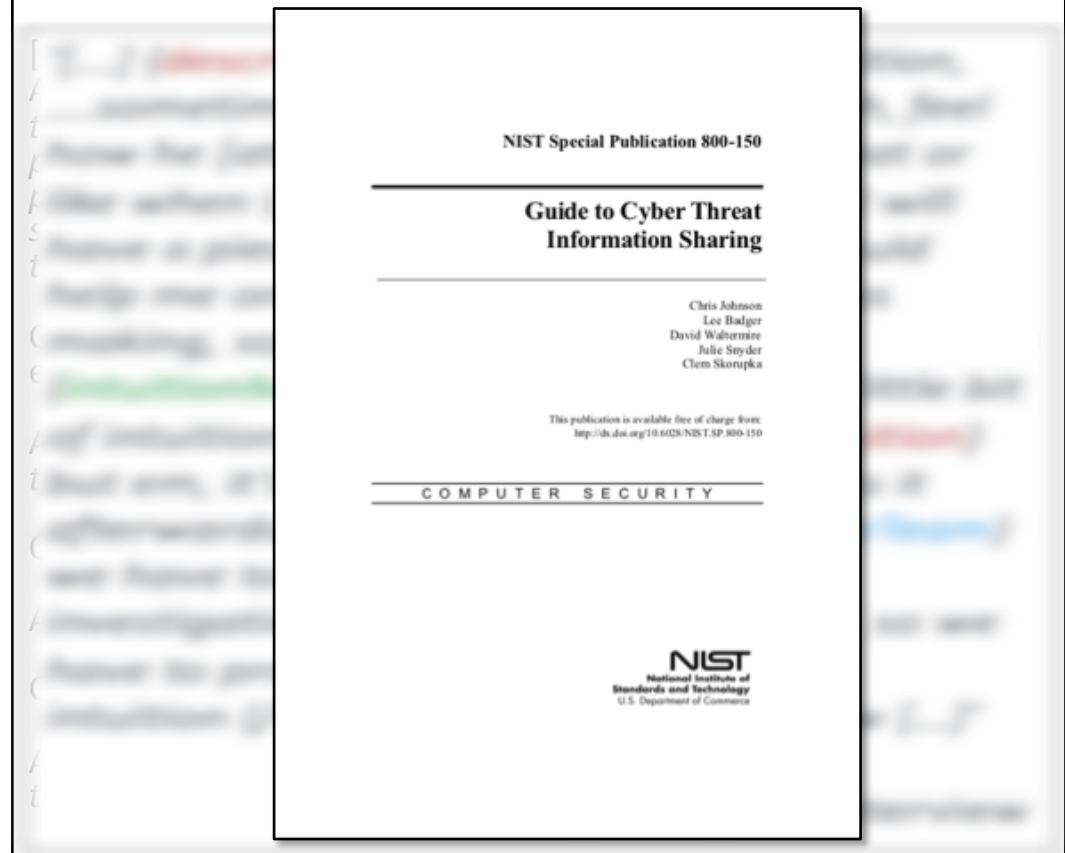


# How people make sense of their world

## 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
- ...

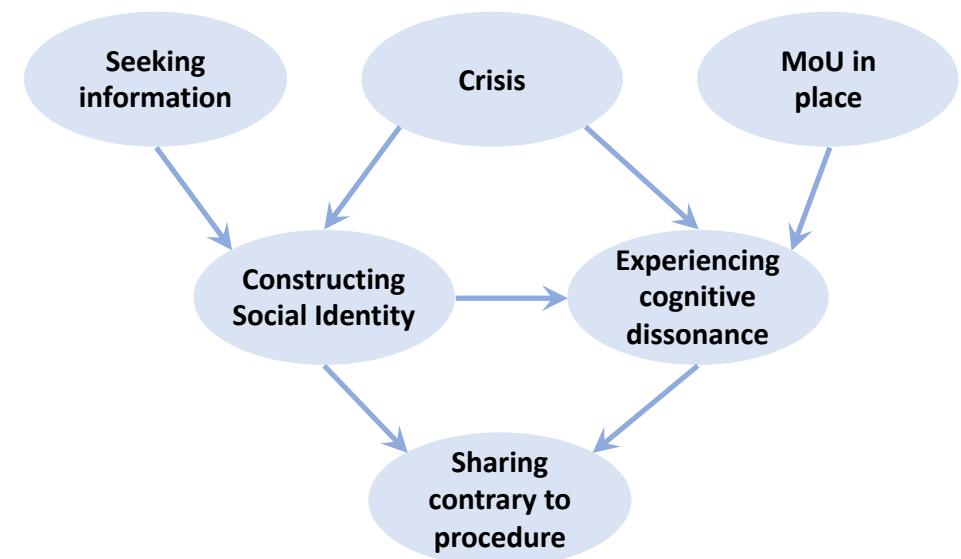
## **Member of a global community**

- 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?

