IT Security: a game of counting the negatives, but can we do better?

From Safety I to Safety II in IT Security

Mate Soos

@msoos@post.lurk.org
www.msoos.org

Based on ideas and inspired by Mario Platt, Sidney Dekker, Erik Hollnagel, Nancy Leveson, and others

A little bit about me

- Doing IT security for ~15 years
- Did many things from chip reverse engineering, pentesting, to cloud security architecture design
- Currently working on formally verifying smart contracts
- Currently doing research on formal methods such as SAT solvers

A little bit about safety vs IT security

Security is not quite safety – in safety, there is nobody maliciously trying to fill your mine with methane and ignite it.

- But there are miners who got tired of the methane warnings & turn them off
- There is management who set production targets impossible to achieve without innovative ways to do it safely
- There are warnings signs, with experienced miners leaving your company due to safety concerns

Thousands of people died in safety accidents. People spent hundreds of man-years figuring out why.

In contrast, IT security mishaps barely get a mention: few good reports, most not in the open (e.g. Equifax, some by Mandiant).

There is enough overlap to learn from safety literature. I strongly recommend you take a peek!

Talk overview

- IT security currently, and its side-effects
- How we could do IT security differently
- A hands-on scenario

IT security currently, and its side-effects

What are the goals of IT security?

No adverse events.

- What is an adverse event? And who is it bad for?
- The company?
- The employee?
- The business partners?
- The customers?
- Unrelated third parties?
- Society?

- **Company**: Liability, liability, and, you guessed it, liability.
- **Employee**: extortion, or feel guilty for “being responsible”* for the adverse event
- **Customers:** Customer data is leaked, their account is drained, etc
- **Unrelated 3rd parties:** E.g. chat logs are leaked and non-customers’ personal information is revealed
- **Society:** we make people fear some technology as a whole

How do IT security personnel help reduce risk?

(Centralized Control Mode, Safety Personnel Perspective)

Safety personnel:

- Support the task-based identification of hazards
- Facilitate the identification and assessment of system level hazard
- Develop controls for tasks and processes
- Monitor controls proactively (e.g. inspections) and reactively (e.g. incident investigation)
- Provide safety incident and compliance reporting to line management and regulators
- Support line management decision-making and arbitrate between stakeholders as necessary
- (Promote an 'authority to stop work' for safety across the frontline workforce)
- Develop and promote safety culture improvement programs

Provan et al: Safety II professionals: How resilience engineering can transform safety practice (2020)

Adaptation of front-line work to rules & controls

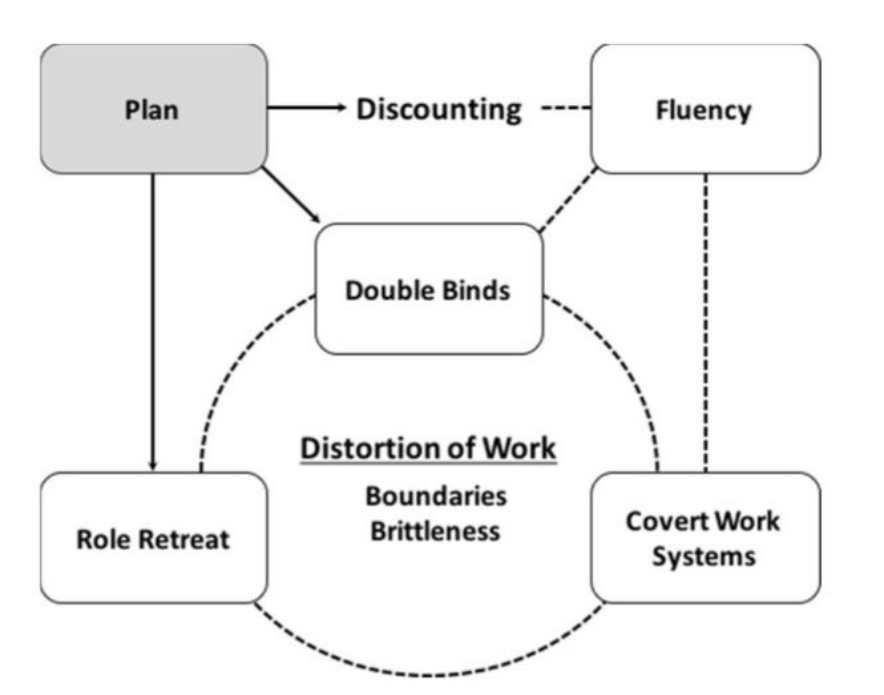
(Centralized control mode of safety)

- **Plan**: Existing strategies, plans, roles, requirements and process that should be applied to activities. To an insider, the expectations and understanding of work never match the reality of what it takes, and how work gets done.
- **Fluency**: Well adapted activity that smooths over contradictions and challenges to make things work. To an outsider, the work seems well coordinated which hides the difficulties that they had to work around to make things work.
- **Discounting**: Problems and issues with front-line work are discounted by management and safety professionals if they are outside of work as imagined.
- **Double binds**: Managers, front-line workers and safety professionals face irreconcilable decisions between two simultaneously necessary but incompatible choices. Neither decision resolves the other issue.
- **Role retreat**: Front-line workers retreat to just performing their role as defined: 'work to role'. This undermines collaboration, especially when things are difficult.
- **Covert work systems:** Work as done is hidden from outsiders due to the fear that it will be stopped or changed. The greater the gap between work as done and work as imagined, the greater the effort that goes into keeping the shadow work systems underground. Work as done has the illusion of alignment with work as imagined through teams dutifully meeting outside expectations through surface compliance activity (i.e. tick and flick, lip-service).

Provan et al: Safety II professionals: How resilience engineering can transform safety practice (2020)

Adaptation of front-line work to rules & controls

(Centralized control mode of safety)



Provan et al: Safety II professionals: How resilience engineering can transform safety practice (2020)

Side-effect: Blame culture

- We go “down and in” rather than “up and out”
- We seek the individual component that was broken: line of code, wrong click (phishing), etc.
- Something bad happened, so something must have been broken
- Furthermore, if something really bad happened, something really big must have been broken.

But…

- What if nothing was broken?
- What if things operated normally?
- What if the attacker just triggered latent failures in our systems?

How we could do IT security differently

If “IT security = no adverse events”, then here’s a radical way of achieving IT security

Don’t use IT systems.

For anything. Ever.

Done! Presentation is now over.

Thank you for your time.

Clearly, “IT security != no adverse events”

So, let’s redefine it.

Here’s a definition:

Everything goes right, all the time.

Since it’s impossible for something to both go right and wrong at the same time, this sounds good. Furthermore, this actually says what we mean: that we get things done using IT systems, all the time.

Safety-I vs Safety-II(Hollnagel)

Safety I	**Safety II**
Learn from Errors	Learn from successes
Safety defined by absence	Safety defined by presence
Reactive approach	Proactive approach
Understanding what goes wrong	Understanding what goes right
Accident causation models	Repeat what goes right
Avoidance of errors	Enforce successful behaviours
Reducing losses	Create new processes based on successful behaviour

Hollnagel: A Tale of Two Safeties (2013) [link]. Also: https://safety4sea.com/cm-safety-i-vs-safety-ii-an-overview

How do IT security personnel help in this mode?
(Guided Adaptability Mode)

Security Personnel can now:

- Explore everyday work. Understand the way the organisation is currently operating and where resilience and brittleness is present
- Support local practices and guide adaptations for safety.
- Reduce goal conflict and negotiate redistribution of resources. Monitor goal conflict and create action to alleviate it.
- Facilitate information flows and coordinate action: create mechanisms to transfer information and coordinate action across organisational boundaries.
- Generate future operational scenarios. Utilise current understanding of the organisation to predict future conditions.
- Facilitate Sacrifice Judgements. Support the understanding of trade-off decisions and the resolution of acute goal conflict.
- Facilitate Learning. Create organisational change based on current conditions and future scenarios.

Provan et al: Safety II professionals: How resilience engineering can transform safety practice (2020)

Looking at the positive brings to light trade-offs

If our goal is to for work to go well all the time, then it's hard to sideline the question of trade-offs.

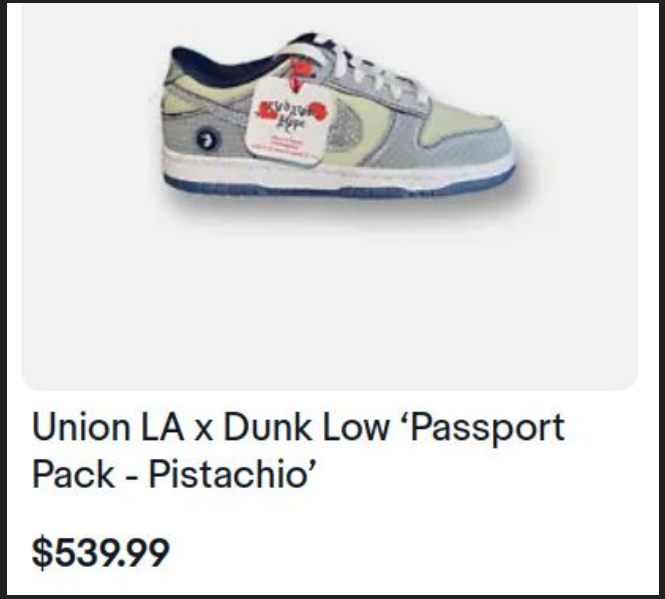
There are always trade-offs made for security. It'd be so much easier to do just telnet into everything, and use no password/authentication at all.

- Not all security rules & systems are net positive. Some may hurt more than they help. Check the contribution of each security rule & system you have.
- How sure are you of the effectiveness of the security rules/systems you have? Have you checked how people go around it? (it's not a question of "if", but "how")
- Have you asked why they go around it? (what double-binds are they in?) Can their go-around be a better trade-off?

A hands-on scenario

Scenario

Attacker used bots to buy up newly released hyped sneakers. However, it was noticed by the people packaging the orders (since they all went to the same address), and the SRE team quickly added a throttle to limit orders

- 

Positive vs Negative slack in the system

What most would concentrate on:

- The missing preparation to hyped articles being sold
- Lack of detection systems for sniping articles
- Lack of reactive measures to throttle sniping

What we tend to forget:

- The people packaging the orders noticed something unusual. Can they tell us something else they have noticed? Maybe they have noticed other weird things?
- SRE did really well! Can we use their systems against other types of attacks?

Notice: “Facilitate information flows and coordinate action: create mechanisms to transfer information and coordinate action across organisational boundaries.”

Safety Currently vs Safety Differently

Safety Currently	**Safety Differently**
People are a problem to control	People are the solution
Tell them what to do	Ask them what they need
Count success by absence of negative	Count positive capacities

Dekker's talk at DevOps Summit [link]

Any questions?

Mastodon: @msoos@post.lurk.org

Email: mate.soos@gmail.com

Blog: www.msoos.org

GitHub: @msoos

References:

- Mario Platt: Security Differently - Insights from RE and Safety (2022)
- Mario Platt's blog at: https://www.securitydifferently.com/
- Provan, Woods , Dekker, Rae: Safety II professionals: How resilience engineering can transform safety practice (2020) [link]
- Sidney Dekker: The Safety Anarchist (2018)
- Nancy G Leveson: Rasmussen's Legacy: A Paradigm Change in Engineering for Safety (2016) [link]
- Sidney Dekker: The Field Guide to Understanding 'Human Error' (2014)
- Hollnagel: A Tale of Two Safeties (2013)
- Sidney Dekker: Drift Into Failure (2011)
- Snook: Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq (2000)
- Rasmussen: Risk management in a dynamic society: A modeling problem (1997)
- Diane Vaughan::The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA (1997)
- Charles Perrow: Normal Accidents (1985)
- Barry A. Turner: Man Made Disasters (1978)