



Practical Magic: Behavior-based Security Design for IoT

Kelly Shortridge (@swagitda_)

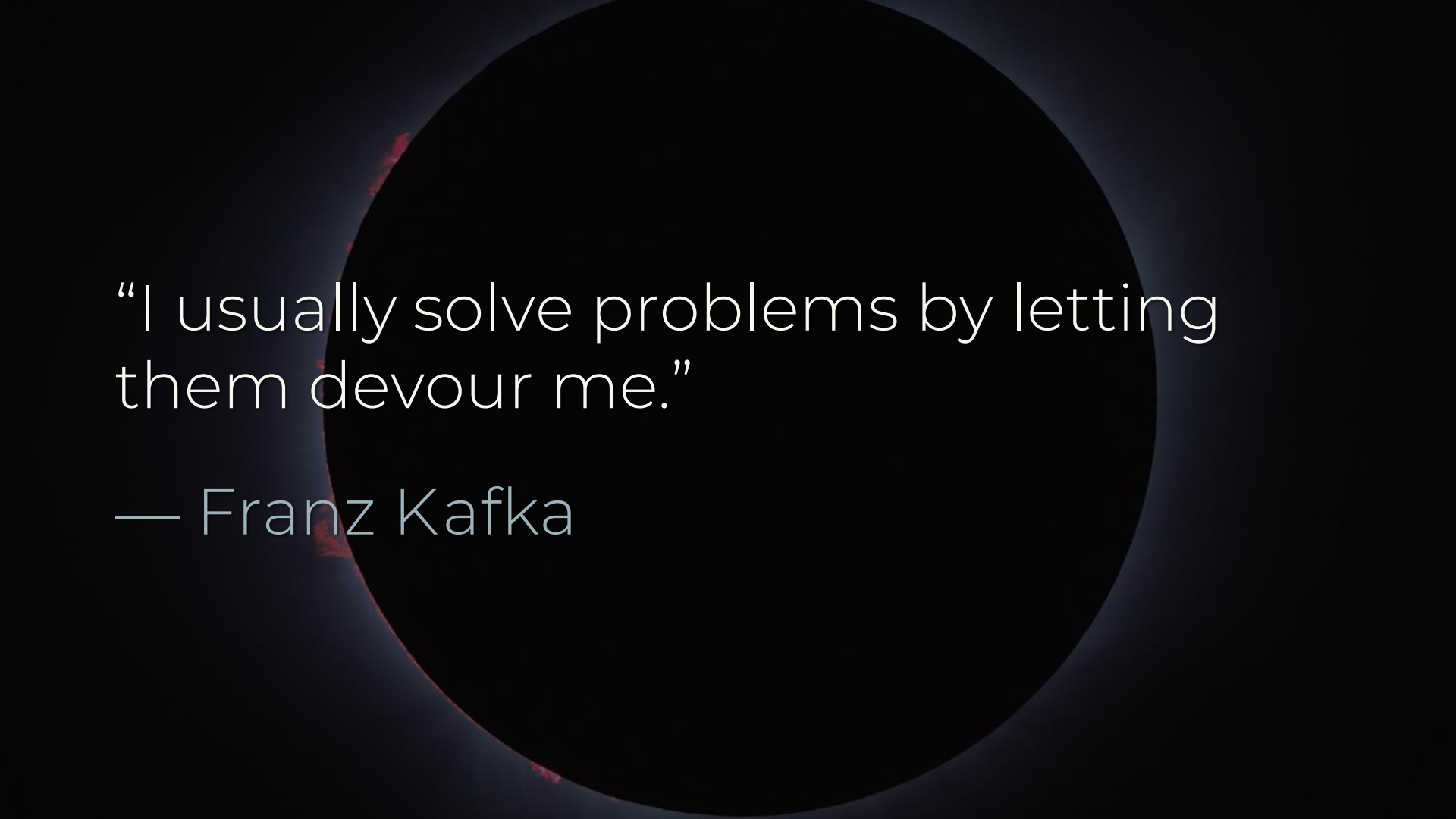
Troopers 2018



Hi, I'm Kelly

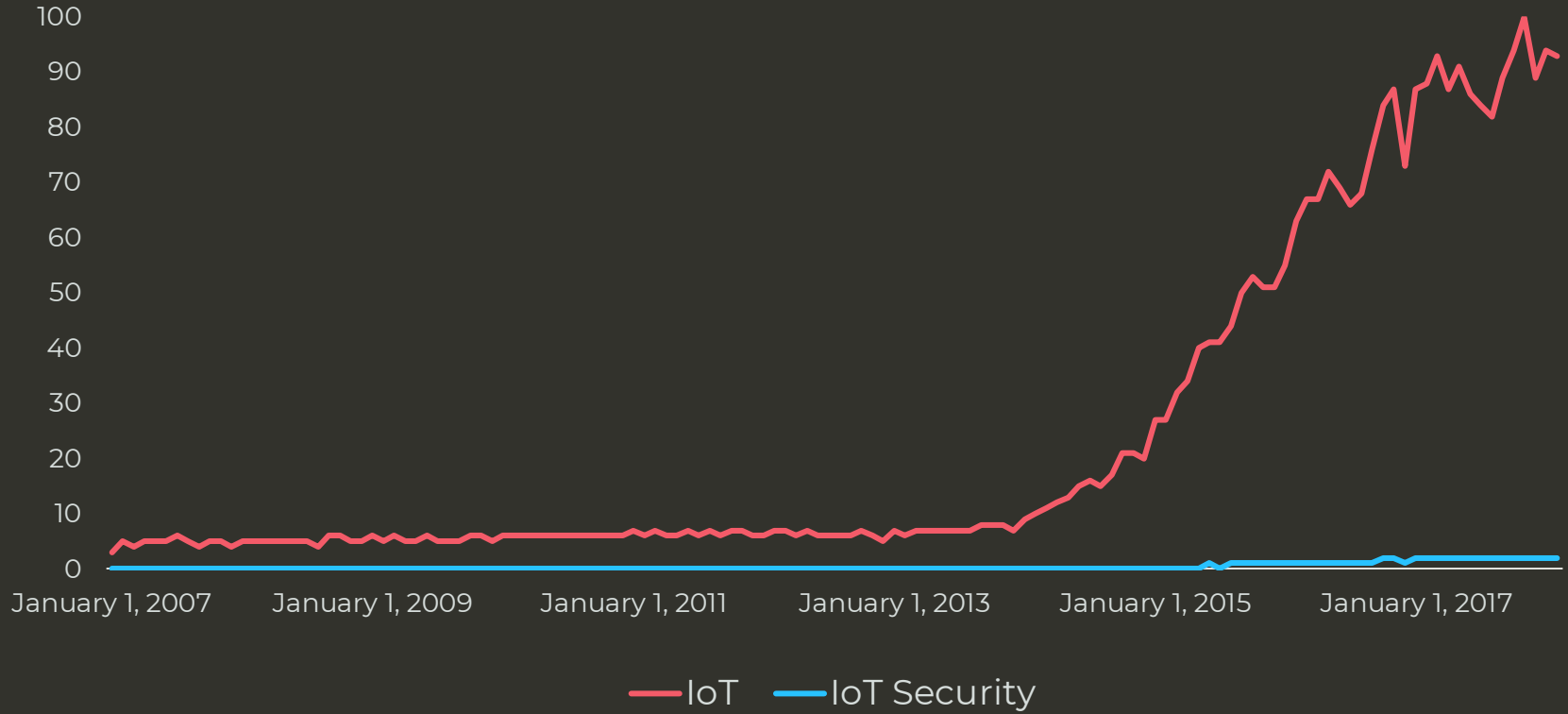


SecurityScorecard



“I usually solve problems by letting
them devour me.”

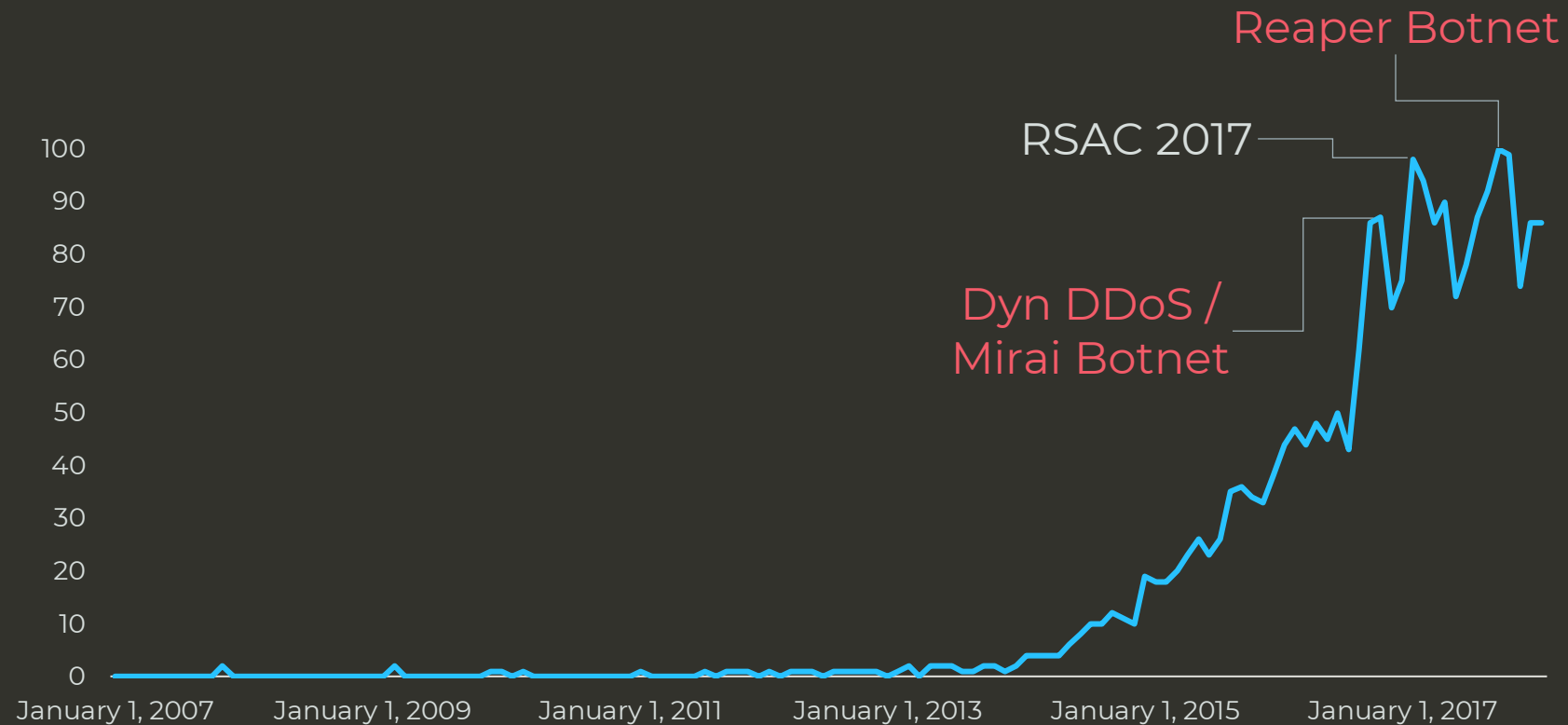
— Franz Kafka



Source: Google Trends



We're engendering a Kafkaesque
paradigm for IoT security



Source: Google Trends



IoT botnets are the first, and ravenous,
boss of the IoT security battle

A large flock of birds flying in a circular pattern against a dark sky. The birds are silhouetted against a dark, overcast sky, creating a dense, circular cloud of movement. The overall scene is dark and atmospheric, with the birds' flight paths creating a sense of organized chaos.

Mirai: 60 default passwords led to
100k node botnet attack against Dyn




But we're promoting complexity & a seemingly endless set of hurdles



Lackluster IoT security is not a secret –
our ideas are clearly not working

A person is performing a yoga pose in a forest. They are in a low, forward-leaning position with their arms extended forward and their head tucked down. The forest floor is covered in fallen leaves, and the background is filled with trees. The overall scene is dimly lit, suggesting an overcast day or a shaded forest.

By understanding behavior, we can
guide choice & support secure habits

- 
1. Existing Suggestions
 2. Incentive Problems
 3. Behavior-Based Design
 4. IoT Security Ideas



Existing Suggestions

FTC recommends building-in security
from the beginning (simple as that!)

FDA: Pre- & Post-Market Guidelines (H/T @marasawr)



Pre-market: a lot of documentation & threat modelling

Post-market: monitoring & a mitigation deployment strategy

OWASP: IoT Testing Guide, IoT Attack
Surface Areas, Principles of IoT Sec...

Designed for the penetration tester
user persona – not developers

A dark, moody photograph of a forest. A prominent tree trunk is in the foreground, showing rough bark with some reddish-brown spots. The background is filled with many other tree trunks, creating a dense, vertical pattern. The lighting is low, giving the scene a somber and mysterious atmosphere.

Cisco's guidelines: "Secure Analytics,"
Network Enforced Policy, Auth²

Compensating Controls: post-market remedies by third parties

A photograph of two hands, palms facing forward, covered in a thick layer of dark mud. The hands are positioned in the lower half of the frame, with the fingers spread. The background is dark and out of focus, suggesting an outdoor setting. The overall mood is one of hardship or struggle.

Burden is primarily on the end user

A close-up photograph of a hand holding a crumpled piece of white paper. The hand is positioned in the center-right of the frame, with fingers slightly curled around the paper. The background is a dark, out-of-focus gradient. The overall mood is one of discovery or revelation.

Actionable, real-time behavioral
analytics for visibility & intelligence...

Maybe feasible for enterprises, but
what are consumers to do?

Incentive Problems





Principal-agent problem: someone else makes the decisions, but you bear the impact

The Agent has their own self-interest.
It's likely not the same as yours.



Moral Hazard: people take more risks
because someone else bears the cost

Next level: Equifax's customers aren't the end users whose data is stored

Prospect Theory: people care about relative vs. objective outcomes

A close-up, dimly lit photograph of a hand pointing to a map. The map is spread out on a dark surface, and the hand is visible on the right side, with the index finger pointing towards a specific location. The map shows various geographical features, including roads, rivers, and a red dashed line. The overall scene is dark, with the map and hand being the primary focus.

Maintain a reference point against
which outcomes are measured

A white feather with a green gemstone set in a dark, textured background. The feather is positioned diagonally across the frame, with the gemstone located near its base. The background is dark and appears to be a natural, possibly stone or wood, surface with some greenish-yellow spots.

Overweight small probabilities &
underweight large probabilities

Overhyping low-probability vuln
exploitation vs. default passwords

A close-up photograph of a person's hand, palm facing forward. The hand is adorned with several rings: a wide silver band on the thumb, a ring on the index finger, and a ring on the middle finger. The person has blue nail polish on their thumb. The background is dark and out of focus.

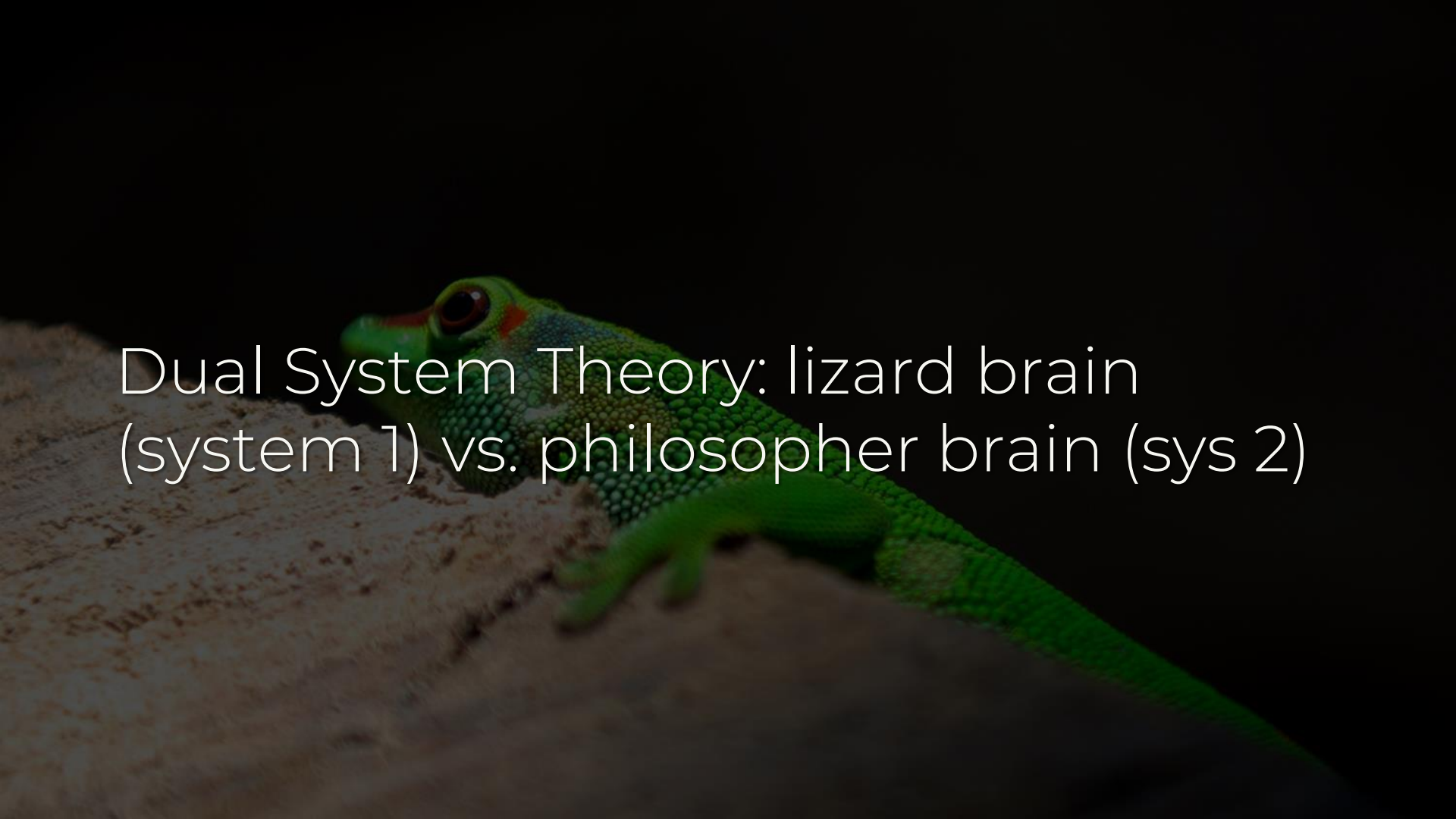
Loss aversion: people prefer to avoid losses vs. acquire the same gain

Framing security as a time & cost sink
facilitates natural resistance



Hyperbolic discounting: future
rewards are discounted vs. present

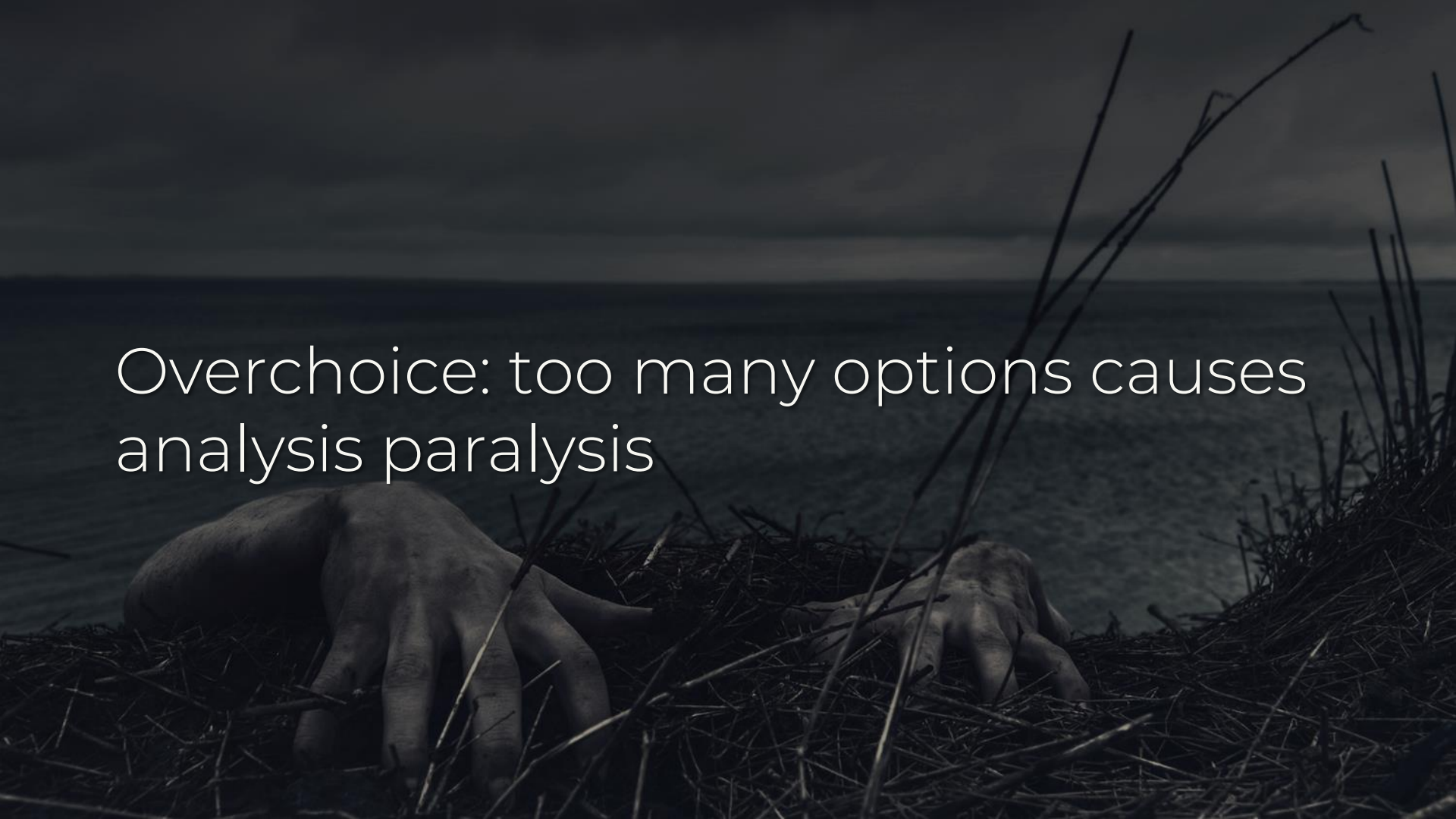
Many security initiatives are
“investments” with long-term benefits

A green lizard is shown in profile, facing left, resting on a light-colored, textured surface. The lizard's body is covered in small, raised scales, and it has a prominent eye with a red ring. The background is dark and out of focus.

Dual System Theory: lizard brain
(system 1) vs. philosopher brain (sys 2)

Most policies work on System 2 – we need to work with System 1 instead

Overchoice: too many options causes
analysis paralysis



Which of the 100 items do devs tackle
1st in a 10-page IoT attack surface doc?

We have to work with how people think, not against it

A top-down view of a person's hand squeezing a lime into a stone mortar and pestle. The mortar contains some ground ingredients, and the pestle is resting inside. The background is dark and out of focus, showing some green herbs. The text "Behavior-based Design" is overlaid in white on the left side of the image.

Behavior-based Design



What is choice architecture?

Design presentation of choices to
promote improved decision-making

Example: MINDSPACE framework for behavioral design

A dark, moody photograph of a riverbank. In the foreground, a discarded plastic bottle lies on a large, dark rock. The background shows a river flowing through a forested area, with a building visible on a hillside in the distance. The overall atmosphere is somber and environmental.

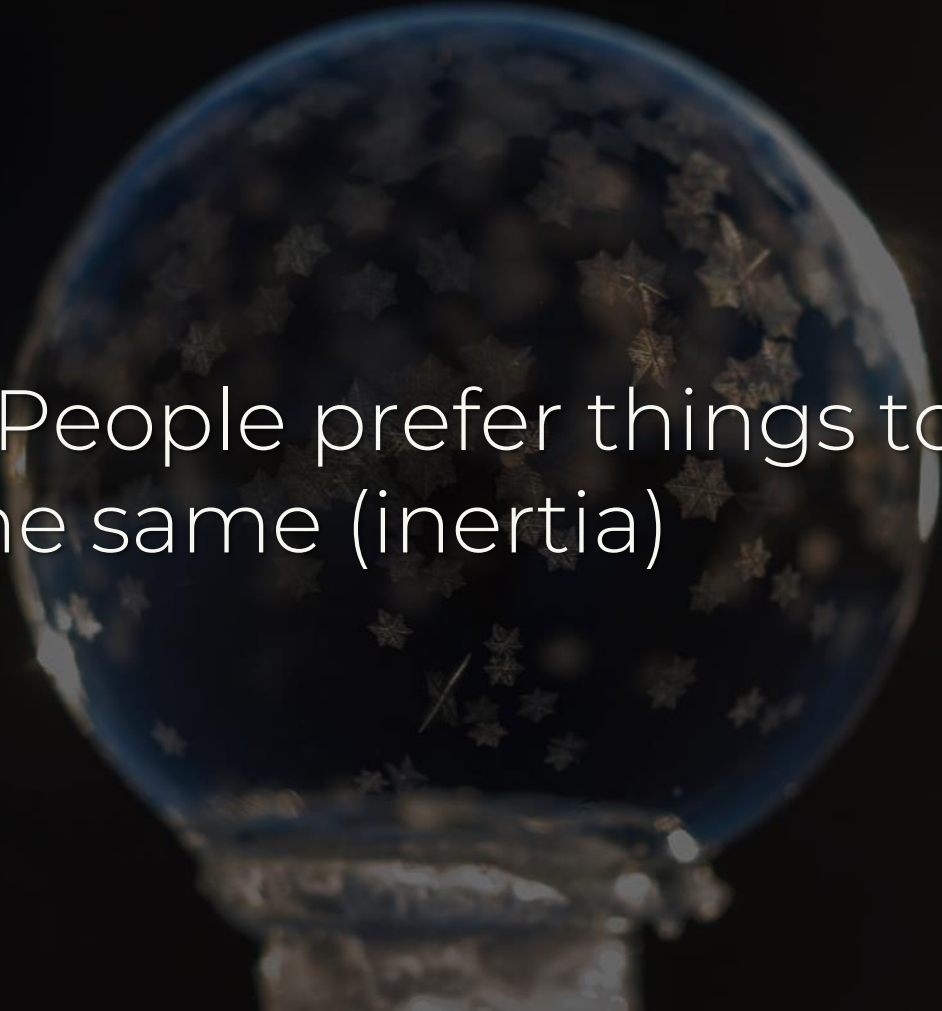
Messenger: people dismiss info from sources they don't like / respect

A close-up photograph of a hand held palm up, with a stream of sand falling from it. The background is a soft, out-of-focus light color. The text is overlaid on the left side of the image.

Incentives: losses can be more motivating than rewards



Norms: People follow social standards,
(even when counterproductive)

A snow globe with a globe of the Earth inside, surrounded by falling snowflakes. The globe is centered in the background, and the snowflakes are scattered throughout the scene, creating a sense of movement and depth. The overall tone is dark and atmospheric.

Defaults: People prefer things to remain the same (inertia)

A vibrant, abstract mask with a complex pattern of red, blue, and green shapes on a black background. The mask has a wide, open mouth and a large, dark eye area. The patterns consist of various shapes, including circles, stripes, and irregular forms, creating a visually stimulating and somewhat chaotic appearance.

Saliency: Novel & relevant draws attention & influences choices



Priming: Senses subconsciously
influence us

A close-up photograph of a black cat with striking orange eyes. The cat is looking directly at the camera with a calm, steady gaze. The background is dark, making the cat's fur and eyes stand out. The text is overlaid on the left side of the image.

Affect: Emotional reactions are our
brains' first responders

Commitments: Judgements made in advance to create “automatic” actions

A person is holding an empty oval mirror in front of their face. The mirror is empty, reflecting only the dark background. The person's hands are visible at the top of the mirror frame. The overall scene is dimly lit, with the mirror being the central focus.

Ego: People like to feel better about themselves & preserve self-image

Reinforcement mechanisms:
consequences to guide behavior

Pay-for-performance lacks empirical evidence for fixing moral hazard

Set clear, achievable goals – “fix all the bugs” is neither

Goal setting must be matched with feedback, ideally immediate



Framing effects: reduce the gap
between concern & willingness to act

Focus on leveraging system 1 to your advantage by altering habits



How do you create a habit loop?

Step 1: Routine



Make it stable, frictionless, & fit into existing context


Minimize perceived effort & number of decisions the user has to make

A close-up, dark photograph of several brass bells hanging from chains. The bells are arranged in a cluster, with some in sharp focus and others blurred in the background. The lighting is low, creating a moody atmosphere. The text "Step 2: Triggers & Rewards" is overlaid in white, sans-serif font on the left side of the image.

Step 2: Triggers & Rewards

Contextual cues: “If X, do Y”

Magical brew of rewards: mix of short-term & accumulated long-term ones

A close-up photograph of a person's hands using a stone mortar and pestle. The person is holding the pestle with both hands, applying pressure to grind the contents of the mortar. The mortar is a light-colored stone, and the pestle is a darker stone. The background is dark and out of focus. The text "Step 3: Ingrain" is overlaid on the left side of the image in a white, sans-serif font.

Step 3: Ingrain

Foster ample opportunities for
practice & interaction

A row of lit candles against a dark background. The candles are of varying heights and are lit, with their flames glowing. The background is dark, making the light from the candles stand out. The text is overlaid on the image.

Cultivate a sense of meaning behind
the habit – a deeper purpose

People don't like feeling like habit machines; play into self-identity

A hand is shown pouring a yellowish liquid from a glass bottle into a stone mortar and pestle. The mortar contains some brown, chunky ingredients. The background is dark and out of focus, suggesting a kitchen setting. The text "Ideas for IoT Sec" is overlaid on the left side of the image.

Ideas for IoT Sec



Set concrete goals: “build-in security”
is too nebulous

“Ensure each feature release uses a 10-point checklist” is a clear ask

Value should consider maximum security benefit at minimum cost

Teams should have a regular, brief time & space to review security goals

A lit lantern is the central focus, positioned on the right side of the frame. The lantern is dark, possibly black or dark brown, with a glass chimney and a metal frame. A single candle is lit inside, casting a warm, yellowish glow. The background is almost entirely black, with some faint, dark shapes that could be leaves or other objects, but they are mostly obscured by the darkness. The text is overlaid on the left side of the lantern, in a clean, white, sans-serif font. The text is centered vertically relative to the lantern's height.

Context cues: “if login portal, require change of default creds during setup”

Specify attainable steps with minimal complexity, like a checklist

Security suitably serves as a deeper purpose – frame it as a noble cause

How can we leverage MINDSPACE for
IoT security?



A woman with long dark hair is lying down in a dark room, her eyes closed. She is wearing a dark top. Several lit candles are visible around her, casting a warm, yellow glow. The scene is dimly lit, with the primary light source being the candles. The overall mood is somber and contemplative.

Find the right messenger: preachy
infosec people probably aren't it

“Gift” budget that is eroded if security goals aren’t met (loss aversion)

The background of the slide is a dense, repeating pattern of monarch butterflies. The butterflies are rendered in a dark, muted color palette, primarily dark brown and black, with some lighter brown and white accents on their wings. They are scattered across the entire frame, creating a textured, almost abstract effect. The text is centered over this pattern.

Treat security habits as norms: “90% of our developers fix bugs within 3 days”

Show long-term expenses of options
to highlight ROI of proactive security

A hand is holding a white Polaroid-style photo frame against a dark, textured background. The frame is empty, and the text is overlaid on it.

Transparency around quality & cost:
easiest measures with highest impact

Control instincts to security issues –
slow down via threat modelling

A close-up photograph of a person's hands holding a large pile of gold coins. The person is wearing a red garment. The background is dark and out of focus. The text is overlaid on the image in a white, sans-serif font.

Team bonus if you complete the checklist & fix bugs within 30 days – if not, it goes to charity

Black Girls Code, Calyx Institute, IFF
Diversity & Inclusion Fund, Mozilla
Foundation, Signal Foundation

Public lists of IoT vendors allowing default cred changes (like the Two Factor Auth List)



One-page checklist to ensure &
document IoT security basics



Streamlined number of steps per
lifecycle stage – design, build, test

1. Design UX workflow to change default passwords (everywhere)

2. Spoof headers to look like most common web servers

3. Encrypt data in transit with SSL or TLS

4. Don't call bash scripts from the web interface

5. Don't use custom API protocols –
just use REST or SOAP

Design

- Does the device use:
 - A login portal?
 - Yes, and we allow the change of default creds
 - No
 - User Data
 - Yes, & we encrypt data w/ SSL or TLS
 - No
 - Web Interface
 - Yes, and we do not call bash scripts or use custom API protocols
 - No

If internet-connected, spoof headers to appear “normal”

Cross-checking by teams of critical measures to be taken

Build

- Share essential information concerning security steps with the team
- Confirm each team member understands the security requirements
- Have any new features been added since design that require review? (ie interfacing w/ the internet, collecting user data)
- Anticipated Security Events
 - What are the critical or non-routine security controls required?
 - How long will implementation of controls take?
 - What are the anticipated impacts of the controls?

Test

- Tester to confirm:
 - Completion of account controls (default credential alerts, lockouts, 2FA)
 - List of data used by the device, and labelling of user data
 - Whether there are any vulnerabilities to be addressed
- For builders:
 - What are the key concerns around management going forward and any future security concerns?
 - Instructions for immediate post-testing security management are drawn up together

Formalized & usable checklist to be released soon...

A dark, atmospheric scene featuring several pumpkins, a skull, and lit candles. The scene is dimly lit, with the primary light source being the flames of numerous lit candles. The candles are of various sizes and are scattered across the foreground and background. The pumpkins are dark and textured, and the skull is a light, bleached color. The overall mood is mysterious and somber.

Conclusion

An hourglass with blue sand is positioned in the center of the frame. The hourglass is made of dark wood and glass, with the sand flowing from the top bulb to the bottom bulb. It sits on a dark, textured surface of small, rounded stones or pebbles. The background is a dark, gradient-like field, possibly a beach at dusk or night, with a soft glow behind the hourglass. The overall mood is contemplative and emphasizes the passage of time.

IoT security ideas must treat devs as
time-constrained humans

A dark, textured background featuring a heavy metal chain with a padlock, symbolizing security and restriction. The chain is made of thick, dark links and is attached to a metal padlock. The padlock is rectangular and has the word "COMMITTEE" visible on its side. The background is a dark, mottled grey with some faint, embossed patterns, possibly of a stone or metal surface. The overall tone is somber and industrial.


Prioritizing security can go against incentives – but that can be changed



Our complex, “endgame-level”
solutions are too formidable

A hand in a grey sweater holds a blue glass over a small fire. The fire is contained in a metal holder, and a thin metal rod is visible. A plume of white smoke rises from the fire. The background is dark.

Compensating controls aren't enough
– we can't expect magic post-hoc



But practical magic using behavioral design can improve decision making

A photograph of a long, narrow tunnel of torii gates, likely at the Fushimi Inari Shrine in Kyoto, Japan. The gates are made of dark wood and recede into the distance, creating a strong sense of perspective. A single lantern hangs from the ceiling of the tunnel. The lighting is warm and focused on the path, with the surrounding areas being in shadow.

Goal: straightforward ways to erode
risky habits & promote security habits



A basic, one-page checklist is a simple way to start growing security culture

A close-up photograph of a white rose in the center, surrounded by flames. The fire is dark and intense, with bright orange and yellow highlights, suggesting the rose is being consumed or destroyed. The background is black, making the white rose and the fire stand out.

We cannot wallow in sermonizing –
we can't let the problem devour us

A circular image of a cracked blue ceramic plate with gold-colored veins. The plate is dark blue with several prominent, irregular, gold-colored cracks or veins running across its surface. The background is a dark, solid color.

“Good enough is good enough. Good enough always beats perfect.”

– Dan Geer

Suggested reading

- “Approaches based on behavioral economics could help nudge patients and providers toward lower health spending growth,” A. Darzi, F. Greaves, D. King, I. Vlaev
- “Behavior-based Safety Guide,” Ireland Health & Safety Authority
- “Farmer Behaviour, Agricultural Management and Climate Change,” OECD
- “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices,” FDA
- “Influencing behaviour: The mindspace way,” P. Dolan, et al.
- “Postmarket Management of Cybersecurity in Medical Devices,” FDA
- “A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population,” Alex B. Haynes, et al.
- “The Theory of Value-Based Payment Incentives and Their Application to Health Care,” Conrad DA



@swagitda_



/in/kellyshortridge



kelly@greywire.net