

Psychology and Computer SEcurity

Technology of Cybersecurity

Seth James Nielson

Psychology is Significant



The Most Powerful Security Tech

Year ago a Dental Hygienist asked me what was the best home security for her computer.

Her question was obviously broad

- Security against worms/vulnerabilities?

- Security against viruses?

- Data security?

Anyone wish to guess my answer?

What is a warrior's Most Powerful Tool?



NO! NO! NO! NO! NO!

This scene convinced me the Jedi were idiots!

It isn't the Lightsaber that made the Jedi so dangerous

Battles aren't won *during* the fighting; they are won in the *thinking* before hand

Weapons aren't you most powerful weapon

What is your *most powerful weapon*?

My answer to my Dental Hygienist?

YOUR MIND!

Your Mind is your Most Powerful Tool

“There is no knowledge that is not power”

(Ralph Waldo Emerson)

Tools serve to ***amplify, not replace***, mental powers

Many effective attacks primarily target the brain, not computers

The Hygienist was disappointed. ***She wanted to not think***

Many want a technology ***that eliminates the need for thinking***

At least at this point, such technology does not exist.

“The real question is not whether machines think but whether men do”

(B.F. Skinner)

Security “Smarts” Won’t Get Better

Some of the problem is human weakness:

- Laziness – don’t want to learn

- Ignorance – lack of opportunity to learn

Bigger problem: *specialization of complex society*

- Nobody can be an expert in everything

- Complex society requires experts to do things

- Harder to self-maintain cars, houses, etc

- Everyone trains, *a lot*, for their specialty

- Little time/energy less for studying something else

What about Out-sourcing?

For our cars, we can go to a mechanic every 15,000 miles

For our houses, we can call a repair service to fix things

For medical, we can have yearly check-ups

Why can't we do this for cyber-security?

The problem is: THIS IS WAR!

Your car is *not trying to break down*

Your house is *not trying to fall apart*

Your body is *not trying to kill you*

Cyber-villains *are actively strategizing about how to attack you*

THIS IS NOT RANDOM CHANCE

THESE ARE HIGHLY MOTIVATED PEOPLE

Solution?



Sounds like Out-sourcing?

Maybe, but please understand the difference

Somebody (or multiple somebodies) must do the thinking

Somebody has to engage in the warfare with the bad guys

Thinking has to be contextualized to the target, not defender

Understand protecting the mind, not just tech/assets

“Only amateurs attack machines; professionals target people”

(Bruce Schneier)

The mind as technology

Forces behind design and development

Intended purposes

Feature set

Strengths

Weaknesses

Contextual requirements

Deployment in practice (intentional or not)

Lessons learned and future directions

How did the Mind Develop?

Evolutionary development of the mind

Higher cognitive functions are very powerful

BUT, have limitations for the pre-historic world

- Can't out think the predator running you down

- Can't think without sufficient information

- Can't think through certain necessary social cohesion

Evolutionary Solution: ***Intuition and Reaction***

Evolutionary Solution: ***DISABLE THINKING***

Understanding Human Cognition

Incorrect: *humans minds are 100% logical and rational*

More correct: *logical thinking often fails*

Example 1: human error

Example 2: human manipulation

Security impact:

Impacts correct human use/deployment of security systems

Impacts correct defenses of the human targets

Lecture Roadmap

Human Error

- Source #1: Automation

- Source #2: Complex Rules

- Source #3: Meta Ignorance

- Source #4: Wrong Model

- How attackers manipulate errors

Human Manipulation

- Attacking human bias (e.g., toward action)

- Attacking emotional fallback

- Attacking via social engineering (e.g., tribal or authority)

- Attacking via visual-emotional

Psychology-aware Security Engineering

The Psychology of Human Error

Many cybersecurity incidents happen because of error

- Giving the wrong access

- Not updating a vulnerable system

Some designers blow off errors as “stupid human errors”

- Condescending attitude of “it’s their own fault”

- Doesn’t understand limitations of the brain

- Doesn’t solve the problem

Understanding *why* humans “fail” can improve design

Source of Error: Automation

We spend a lot of time *not thinking*

When performing a skill:

- Very conscious during the learning phase

- Eventually shifts to automatic operation

- Example: Driving

“Slip and capture” errors: wrong automated task

Dangerous to assume a person is thinking

Source of Error: Complex Rules

Some errors happen even while thinking

Humans can consciously choose *the wrong rule*

Impacted by complicated hierarchies:

- More general rules verses more specific

- Rules that change the rules

- Edge case rules*

User doesn't recognize error because "followed the rules"

Dangerous to assume a person follows the right rule(s)

Source of Error: Meta Ignorance

Humans sometimes struggle to ask for help

They either:

- Don't **know** how much trouble they're in

- Or, are **pressured** to act anyway

For example, cybersecurity is hard because it is **abnormal**

- Up until the attack, everything looks/feels fine

- When trouble starts, can be unpracticed getting help

- Cryptography is also an example

Dangerous to assume correctly skilled people are acting

Source of Error: Wrong Model

Everything we “think” is based on models

We cannot understand or know every possible detail

Models help us understand, compare, predict, etc

Models of things: *chair, car, window*

Models of people: *spouse, friend, co-worker*

Wrong Model Error

- Incorrect or incomplete model

- Application of wrong model altogether

Dangerous to assume a person is using the correct model

Note about Civic Discourse

One of the real challenges with healthy, respectful discourse in politics, religion, and other sensitive subjects is an inability to figure out ``the other side's" modeling. If you find there are a large number of people that seem to take a point of view you just cannot understand, it may be worth exploring the models that you and they are using. Working to understand and explain your model, and figure out theirs, can lead to better mutual understanding and an improvement in working others.

Refusal to Abandon Wrong Models

This is another “wrong model error” problem

It appears to be human nature (pride, ego, etc)

Unfortunately shows up in the justice system

Officers become convinced of a “theory” (*model*)

Prosecutors don’t change their minds after DNA evidence

WRONG MODEL ERROR!

The recurring theme of these cautionary tales—and the dynamic on which this article will focus—is the prosecutor’s tendency to develop a *fierce loyalty to a particular version of events*; the guilt of a particular suspect or group of suspects. *This loyalty is so deep it abides even when the version of events is thoroughly discredited, or the suspect exculpated*. It results in a refusal to consider alternative theories or suspects during the initial investigation, or to accept the defendant’s exoneration as evidence of wrongful conviction.

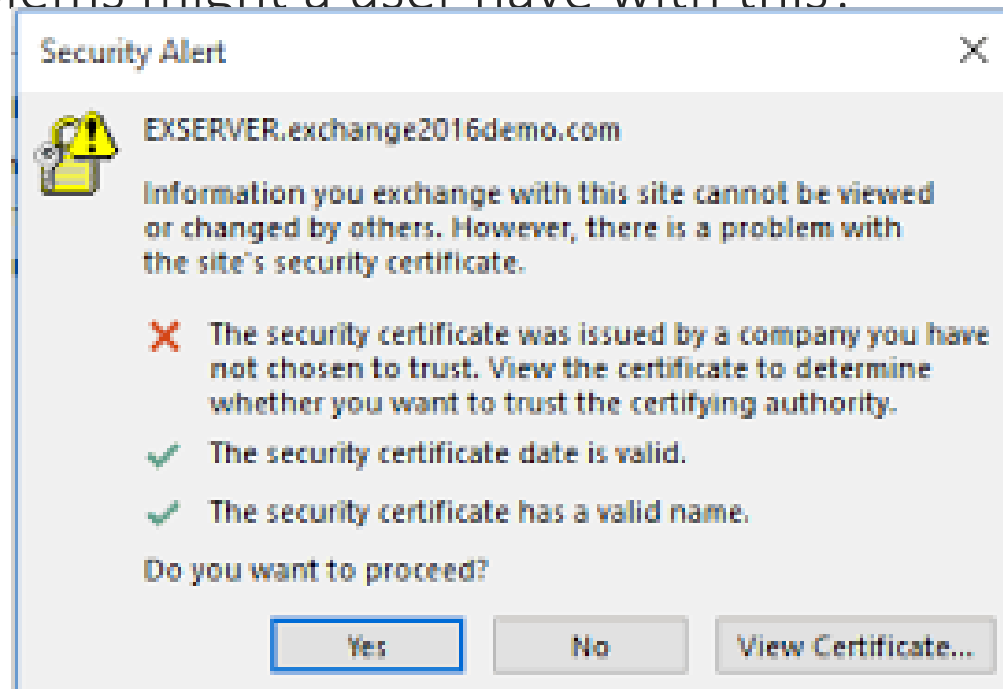
Attacking Humans via Human Errors

Attackers often want to ***control*** the target's behavior

If attackers can induce an error, may lead to desired behavior

Example, redirect a user to a fake website

What problems might a user have with this?



Attacking Machines via Human Errors

Many systems are error-prone already

Attacker need not directly manipulate to induce the problem

For example, many devices ship with default passwords

Users are supposed to change the password before deploying

But many don't. This was used to create a “bot net” in 2016

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Psychology of Manipulation

To repeat: attackers want to ***control*** target behavior

Even if attacking a system, want defender behavior ***predictable***

We all like to think we're too smart to be tricked.

ALL Human minds have vulnerabilities (yours and mine too)

Understanding these limitations leads to solutions

Human Bias Toward Action

Humans are designed with a bias toward action

There are GOOD reasons for this:

- If we thought about everything we'd never do anything

- Can lead to an initial action with follow-up refinement

But there are some very BAD consequences

- Act without sufficient information is sometimes worse than not acting

- In the 21st century, there is a lot of information required to act

- This is especially true in cybersecurity

A word about “bias”

Bias has a negative connotation (e.g., racial, gender, etc)

Bias means *preferences* that are automatic, not based on study

Bias is an essential part of life for basic function/operation

We accept as an axiom that some biases are immoral

Through social/other training, can increase/reduce biases

This is probably also evolutionary

Exploiting Bias

If an attacker knows/predicts bias, can predict human behavior

Serious problem:

- A “good” bias might lead to the “right” decision 99% of the time

- Attacker will still figure out how to exploit the 1%

With action bias, attacker knows that urgency leads to action

If the target believes the urgency, will act unless trained

Commonly seen in phishing

Emotional Fallback

Pushing someone out of logical thinking into emotional response

Can be explicitly triggered through emotional statements

Can also happen when the target “runs out” of logic

This appears to also be evolutionary

We cannot know or reason through everything

What should we do when we don't know what to do?

People often call this “intuition”

Intuition

Intuition (gut feel) only works with evolution (lots of time!!!)

Humanity has not had time to evolve with the technology

Complexity is accelerating (this will continue to get worse)

Exploiting Emotional Fallback

Extremely emotional language triggers emotional responses

Anterior Cingulate Cortex

Reciprocal Repression Model

Emotion shuts down Logic

Push the target to the “edge” of training

No matter how well trained, always something unknown

Attacker will almost always know more than the target

Social Engineering - Trust

Obtaining unauthorized services through false pretenses

Often obtained in stages, across multiple targets

Build a small degree of trust, then leverage for more trust

Common tricks to build trust:

- We're part of the same group: gossip, banter

- I'm already part of the system: I know how it works

- You can help me out: I need you

- I can help you out: you need me

Social Engineering - Authority

Thinking also tends to shut down in deference to authority

Of course there are examples during war time

But how many of us have deferred to social authority?

Ironically, “rejecting” authority is often deferring to ***other*** authority.

Example Abuse of Authority



Let's analyze this Scene

Dead Poets Society was a whole movie about learning to think

Yet, here in a key scene, how does this teacher convince

Thinking? Analysis? Debate? Discussion?

No. He uses emotional statements and emotional activities

He doesn't accept any opposition.

Students ***required*** to think the way he does

Visual-Emotional Stimulation

Our visual processing system is complicated

Pattern matching, video smoothing, etc

But also, there is *emotional* processing in it as well

Man with brain damage studied for his issues in this

He could *recognize* his parents

But it didn't feel right.

Convinced they were *imposters*

We feel when we see things

Attackers attempt to manipulate with *emotional visuals*

Visual Stimulation Example

This was a phishing submission from a previous class

It “got” me

Updating Direct Deposit



Ellie Daw <Ellie.Daw@crimsonvista.com>

1:16 PM

To: Seth Nielsen <Seth.Nielsen@crimsonvista.com>

Hi Seth,

I recently switched banks and need to update my direct deposit information. My new bank account information is:

Acct #: 9089273541

Routing #: 011401533

Please use this account to deposit my next paycheck. Thanks.

Best,

Ellie Daw
Research Scientist
Crimson Vista
Main: (512) 387- 4310
Ellie.Daw@crimsonvista.com
www.CrimsonVista.com

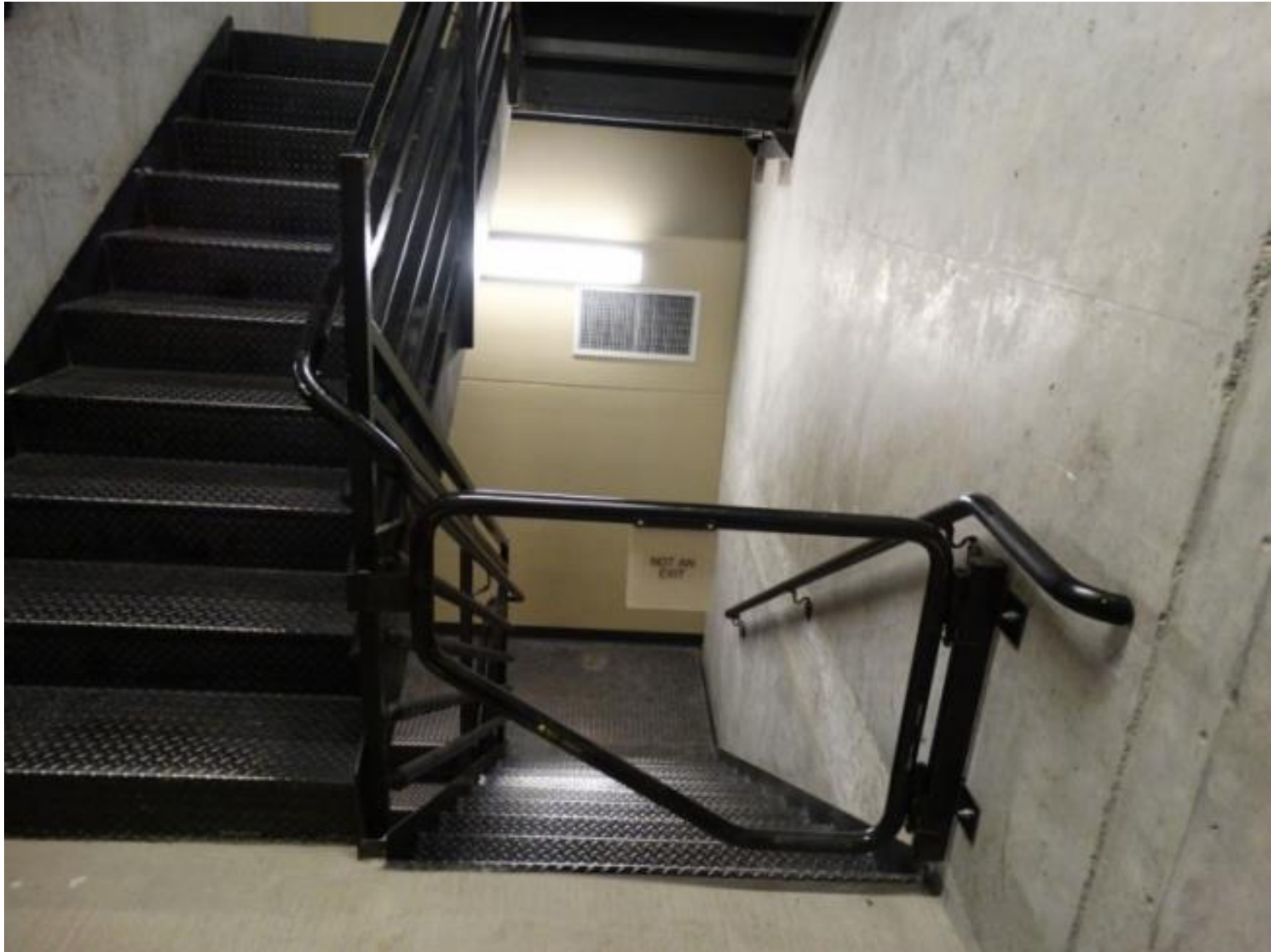
Psychology-Aware Design

First, recognize that everyone is, in fact, human

Design to *mitigate* human weaknesses

Build on human psychology rather than fighting it

An example of Good Psychology



Why is the psychology good?

ASSUMES that the human will panic!

Understands that they just need a mild cue to go the right way

No training required, expected

NOTE: still dealing with fires, which are not conscious enemies

Six Psychology-Aware Design Points

Affordance – Design for proper thinking/use

Modes for irrational user behavior

Inhibit emotional response (logic inhibits emotion)

Design to be resilient in the face of mistakes

Design to be resilient to failures

Pushing decisions to experts

Security Example: CAPTCHAs

Good case study!

Combine psychology, usability, and system design nicely

Designed around what humans do well that computers do not

“Completely Automated Public Turing Test to Tell Computers and Humans Apart”

Thanks Alan Turing!

