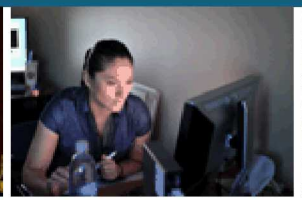
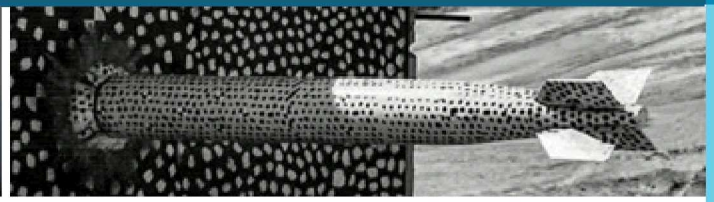
SAND2020-1668C

Application of a simplified process to Identify and Manage Sensitive Digital Assets





Michael T. Rowland

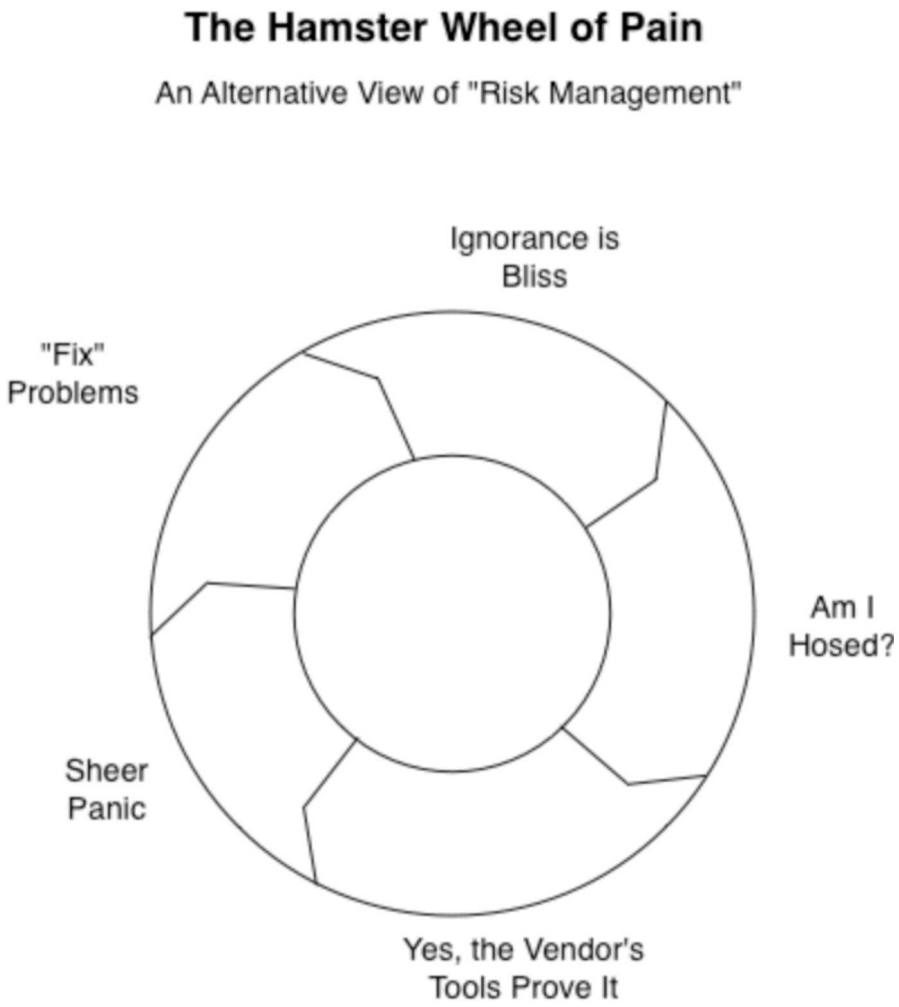
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Challenges with the Asset-Centric Approach

- IAEA NSS 13 para 4.10 provides for a function-based approach:

> "Computer-based systems used for:
> - physical protection
> - nuclear safety
> - nuclear material accountancy and control
>
> should be protected against compromise consistent with the threat assessment or design basis threat."

- Implementations have focused on protection of assets (CDAs), not functions.
- Why is this a problem?
  - This approach limits risk treatment options to:
    - Modify likelihood (by applying computer security measures)
    - Retain risk/risk acceptance
  - Better options:
    - Avoid risk
    - Modify the consequences to reduce harm



Ref. Andrew Jaquith, *Security Metrics, Replacing Fear, Uncertainty and Doubt*, © 2007 Pearson Education Inc.

Simple Analogy - Password

Password Function:

A **password** is a string of characters used to ***verify*** the ***identity*** of a user during the **authentication** process https://searchsecurity.techtarget.com/definition/password

Strength of Password:

Entropy is used as a measure of the strength of a password generator. Increasing the **entropy** of a password generator makes the passwords it creates more difficult for an attacker to guess.

A password generator with an **entropy** of 42 bits is as strong as one which generates a string of 42 bits chosen randomly.

Example requirements for a strong password:

- Password length should be at least eight characters long – the longer the better.
- Password should contain characters from all of the following four sets:
  - lower case letters ('a' – 'z')
  - upper case letters ('A' – 'Z')
  - numbers ('0' – '9')
  - special characters ('!', '@', '#', '$', '%', '&' …)

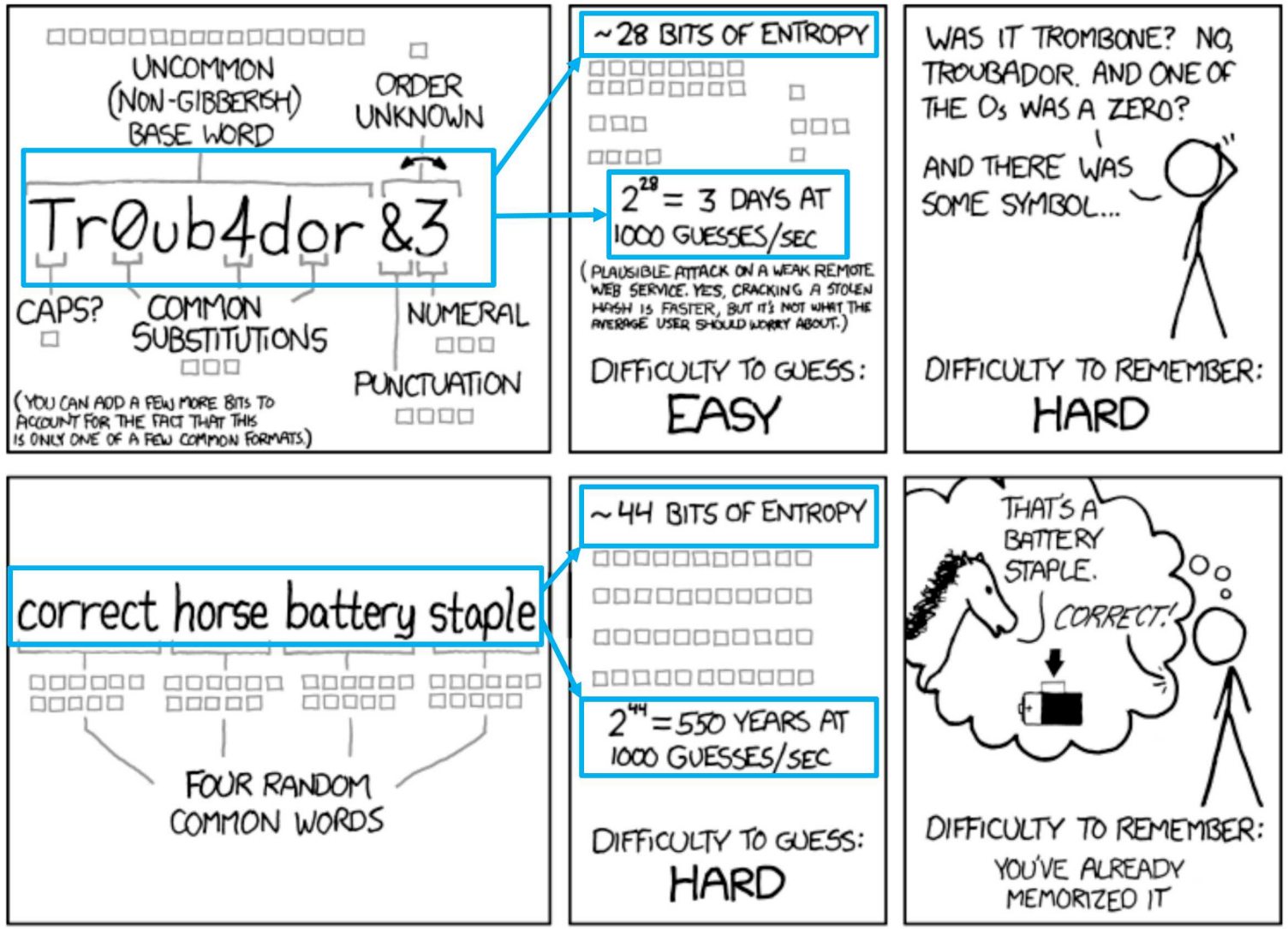
Implementation:

- Password 1: Troub4dor&3
- Password 2: correcthorsebatterystaple

Password 1 meets both the requirements, whereas password 2 only meets the first requirement.

Which password takes longer to guess?

Password Strength – Defender's Point of View



Warning: Do not use "correcthorsebatterystaple" as a password because it has been added to dictionaries used by automated password guessing software.

Ref. Randall Munroe, https://www.xkcd.com/936/

Password Strength – Adversary Point of View

Using Open Source Software (John the Ripper, Cain and Abel) an adversary can easily:

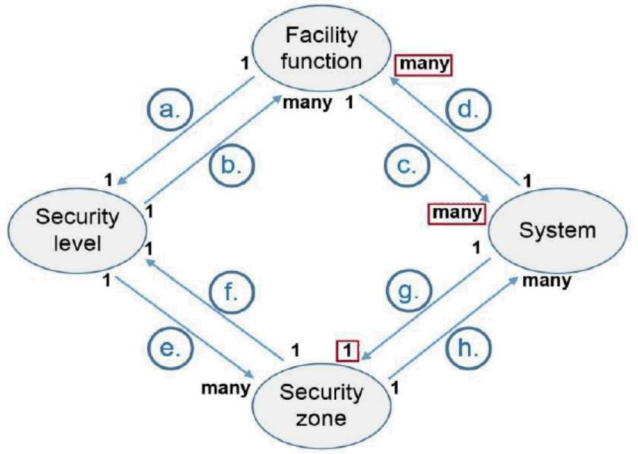
- Brute Force Attack – leads to an equivalent valuation of password strength
- Dictionary Attack – with concatenations of characters and common substitutions based upon knowledge of password policy – leads to an equivalent valuation of password strength as "Tr0ub4dor&3"
- Dictionary Attack – with concatenations of common words – **reduces** the password strength substantively, and dependent on when the correct attempt is made.
- Rainbow Tables – pre-computed Dictionary attacks – **reduces** the level of effort (time) even further if the table is available and previously computed.

The Problem is addition of characters (assets) is decreasingly effective, whereas changing the authentication "system" can **avoid** degradation of strength

For example, adding use of salt ('random number used as an additional input to password hash computation') eliminates the effectiveness of Rainbow Tables.

The objective is to secure and protect the function (authentication) over the system (password) and components/assets (characters in password)

Lessons Learned from Nuclear Safety



Nuclear Safety is a priority process within Management Systems at nuclear power plants.

Functions are paramount

Systems that perform functions need to be systematically conceptualized, designed, developed, fabricated, installed, commissioned, operated, and decommissioned in a way that maximizes reliability and performance.

Safety functions associated with the highest consequences demand the greatest effort (i.e. graded approach).

Safety functions need to be independent and diverse to the greatest degree possible, within a strict framework for deployment based upon plant states (e.g. Architecture, Defense-in-Depth)

Categories of I&C Functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3

Ref. Figure Top Right – IAEA NST047 – Computer Security Techniques for Nuclear Facilities, Draft, TBP
Table: CORDEL Digital Instrumentation & Control Task Force, Safety Classification for I&C Systems in Nuclear Power Plants - Current Status & Difficulties

Difficulties in applying safety processes to security

Nuclear Safety processes were designed to protect against safety hazards, not an intelligent adversary.

Computer Security for Nuclear Security has diverse goals (for example):

- *Safety* – Control of reactivity;
- *Safety* – Removal of heat from the reactor and from the fuel store;
- *Safety* – Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
- *Physical Security* – protect against the unauthorized removal of nuclear material
- *Physical Security* – protect against sabotage resulting in unacceptable radiological consequences (URC)
- *Information Security* – protect against the unauthorized disclosure, alteration, modification, destruction or denial or use of sensitive information

These different goals require different programmes.

But these programmes require monitoring and control via a common management system to ensure that goals, actions, and activities are appropriately prioritized. (i.e. Cyber Security Management System)

Comparing Nuclear Safety and Proposed Approach

Process	Safety*	Proposed Approach (CSMS)
Establish Design Basis (Management System)	Basic understanding of plant design, its safety analysis and how main safety functions will be achieved	Understand security goals, their security analysis, and how the main security goals will be achieved
Inherent Value of Functions	Identification of all functions necessary to achieve main safety functions	Identification of functions that implement, support, or assist in realizing the security goals
	Categorization of all functions	Assign a security level to all functions based upon the potential consequence (i.e. the harm that could occur if the function is not provided when needed, or if the function has been maliciously modified)
	Identification and classification of systems, structures, and components	Identify the digital assets (or systems) that perform or support these functions and assign a security level to the digital assets based upon the contribution that the digital asset provides to provision of the function (i.e. directly performs function, directly supports the function, or indirectly supports the function)
Fault Tree Compromise Analysis of functions	Identification of design provisions to prevent accidents	Evaluate the effects of compromise of functions using an adversary profile and characterization
	Identification and classification of SSCs implemented as design provisions	Identify and assign a security level to the digital assets based on effects of compromise
Decision	Is the classification correct and complete? i.e. The Inherent Value and the Fault Tree Value are identical	Is the security level assignment correct and complete? i.e. The inherent and the compromise value are identical. If not, assign the level requiring the highest protection
Selection of Measures	Select applicable engineering design rules	Select applicable cyber security control methods

* *Safety Standards, Safety Classification of Structures, Systems, and Components in Nuclear Power Plants*, Specific Safety Guide No. SSG-30, IAEA, Vienna, 2014

Conclusion

Computer security programmes (CSP) need to be strategic and intuitive.

CSP policy and requirements need to be flexible, appropriate, and specific to the security goal and to the functions that they are protecting.

CSP should make it easy for humans to understand and confirm the required actions, and how these lead to better security.

Risk treatment should prioritize avoidance of risk and minimization of consequences over the "Hamster wheel of Pain" approach of continual application and update of 'bolt-on' security controls.

Consideration of these points will lead to:

- greater implementation of security by design, and
- a more accurate quantification of the value of functions and the assets/systems that provide them.

Thank you!