The Value of Information

Albert Carlson[*], **Benjamin Williams**[†], **Sai Ranganath Mikkilineni**[‡], **1st Lieutenant Mandeep Singh**[§]

[*]Chair for Entropy and Encryption, Quantum Security Alliance
[†]Department of Computer Science, University of Idaho, Moscow, ID, USA
[‡]College of Business, Delaware State University, Dover, DE, USA
[§]Technical & Information Support Company, 1st Special Forces Group (Airborne), US Army
Email: [*]LtZap1@gmail.com, [†]will9847@vandals.uidaho.edu, [‡]smikkilineni@desu.edu, [§]mandeep.singh35.mil@army.mil

Disclaimer - The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

***Abstract*—Information has value, and this is why people do research, why they can create new and revolutionary products that drive the economy, why hackers target people in identity theft attacks, and why intelligence agents of various countries seek it. Most users do not understand that information has a varied value over its lifetime and is often monotonically decreasing. Based on Shannon's work in the 1940s, information technology indicates that information value can be quantified and predicted. Knowing how information value changes is vital to efficiently protecting that information. This paper discusses the types of information, models for changes in information value, and how to evaluate and adequately understand the impact of time on secrecy and apply that data for appropriately protecting the information.**

***Index Terms*—Information, Believability, Value of Information, Information Theory, Everlasting Security, Opportunity Costs, Time Value of Money**

I. Introduction

Claude Shannon, the father of modern encryption [1] and information theory (IT) [2], stated that information could be measured. Further, he noted that information value monotonically increases as the body of data in a message increases. This fundamental concept is more succinctly stated, "Information is valuable and powerful, including personal information. Be aware of what you are sharing" [3]. If something has value (utility [4]), then an estimate of its value can be assigned in some currency [5]: money, resources, time, importance, or even liability. Value, like utility, varies by the person or organization using (or needs) that particular information. Value also varies across time. Identifying the value of the information is an essential step in adequately and economically protecting that information through methods, such as encryption [6].

Information value is crucial in estimating the appropriate level of security required to secure the corresponding information asset. Attackers know the value of what they are attempting to uncover and have a use for that information. Users must understand the damage their information can cause if it is prematurely revealed to an adversary. The value of information can change based on its environment and the time until it is naturally revealed. Information is an asset with a definite value, though often viewed as intangible. This is not true, as multiple companies claim "trade secrets" [7] and will expend large sums of money to maintain that information as a secret, making them virtually tangible. Military organizations have recognized this value too, protecting their information using encryption and trusted couriers for millennia [8]. Over this time, users have assumed that this information retains its value in perpetuity. However, such is not the case. Information value changes over time until it reaches a minimum value associated with its use or historical role.

A. Related Work

The concept of something having a variable value is not limited only to information. Clues as to how to study and treat a problem can be gleaned from work in other fields with similar or identical mathematics [9]. For this problem, the key characteristics are time variance, a distinct event, and monotonicity.

A related field of study is known as the "time value of money" [10]. This concept addresses how there is a difference between the present value of money and the value of money in the future. This concept explains why taking an upfront, lump sum payment is often more advantageous than splitting the sum into future, smaller payments. Included in this concept is the idea of interest and why it is charged in loans and installments. Interest is the measure that compensates for the loss of value over time. It is applied using the technique of compound interest, which implies that the loss is of exponential shape. While interest and loans recover the loss, the problem of the "opportunity cost" [11] of spending money, the costs of spending money versus paying for something later, is more closely related to information loss. Opportunity costs are not limited solely to money, but can also be used to make choices between any two alternative uses of resources. In both cases, information can be substituted in the same role as money.

B. Outline of Remainder of the Paper

This paper focuses on how information can be characterized and predicted. Predicting the value of that information is important for cybersecurity, believability, and selling/buying information for use. The paper is organized as follows. Section

II introduces the problem of varying information values. Also, it suggests a way to model the value so that the model can provide enough data to affect a security solution. Section III covers the essential information loss models and the information value phases. It also addresses some variations that can affect the model and cause the model to stray from acting in the same manner as the ideal abstractions of value reduction. Section IV discusses how the model is applied to cybersecurity. Understanding the models and how they apply to information security is critical to selecting the correct encryption to protect that information. Choosing the wrong model can result in prematurely revealing the information, spending too many resources, or increasing the cost of keeping the information secret. The final section, Section V, is the conclusion and discusses possible future work on the subject.

II. Models of Information Value Loss

Information value changes according to several models based on the type of information in question. There are three definable phases of information value change:

- Pre-discovery (P)
- Rise (R) (not a phase, but an event)
- Defense (D)
- Equalize (E) (not a phase, but an event)
- Long-term Value (A)

Although the change in the value of the information across assets is not identical, these phases can be considered standard across the assets. However, each phase might not uniformly align across different assets.

The asset may have value before the information is needed, but its importance is limited. This is the Pre-discovery (P) phase (In the figures, the area marked "P" precedes the rise in value). In the next stage, the need for the information is realized, and its value rises to the maximum. The following figures show this by the sudden value rise, which is not an area per-se but an event signified by the rising line. Most, but not all, data monotonically declines in value over time. How the value declines is vital in selecting the suitable encryption algorithm to protect the data. In the figures, this is the area between the lines, denoted by "D". Finally, the long-term value phase is when the damage due to the premature release of the information is limited, and the value during this phase will help decide if everlasting security [12] is needed to protect the information. This area is denoted in the figures by the "A". Understanding the relationship between the information asset and its value model is critical to appropriately protecting it.

A. Model Stages

Information, like energy, has a conservation law. For information, that law can be summarized as follows: information can neither be created nor destroyed, only forgotten and (re)discovered. This law is so essential that Hawking had to revise his early work on the universe to account for it [13].

As discussed above, there are three distinct stages in the life of information value. They are:

- P - The phase that is pre-disclosure or discovery of the information. In this phase of information life, the information has not been discovered or is under development. The information may not be needed for much of the time covered in this phase. The end of the phase occurs when the information is discovered or developed and can be applied to a problem.
- D - The defense phase of the information. This is the phase when the information starts requiring security to avoid premature release. This is also when the information loses value from discovery or recognition until some event. The shape of the curve is vital because the decline allows for calculating the damage at any point between information discovery and an adverse event (like premature reveal). The costs incurred due to an adverse event can include the recovery costs, desired profit for new technology, control of the technology through patent or copyright, or the limit of possible loss/damage associated with the information.
- A - The asymptotic lower limit of the value of the information. Practically, some information value remains at the end of the defense phase. This may only be a historical value and might come close to 0 or settle at some other relatively lower value. After a non-adverse event (like a natural/intended release of information) related to the information occurs, that value is reached and stays relatively constant.

The sudden rise between P and D occurs because the user discovers and knows the information. The boundary between D and A is an equalizing (E) event to which the information value is related. The asymptotic value for the information is the minimum value of the information from that point onward and is reached somewhere between the equalizing event and infinity (i.e., across time). Various models describe the decay of information value. Four major models are now described.

B. Constant Value, or Step Function

The most basic function describing value associated with unvarying information is the Heaviside step function [14]. Once identified, the information retains its value at the same level for all time. The mathematics for this case are relatively simple. After the information is revealed, $\forall t = x$ where $x \geq e_0$

$$v(x) = \begin{cases} 0 & \text{if } x < e_0 \\ K & \text{if } x \geq e_0 \end{cases} \tag{1}$$

Unchanging information, which is needed to build products and calculate other information and falls under the umbrella of facts, theorems, and constants, always retains its value because it is necessary for ongoing problem-solving. This data is often recorded for reference and shared among scientists and engineers.

Figure 1 shows a graph of the value change for this type of information. Depending on the difficulty of finding the information and how critical the information is to the end product, this data may require everlasting security. Another

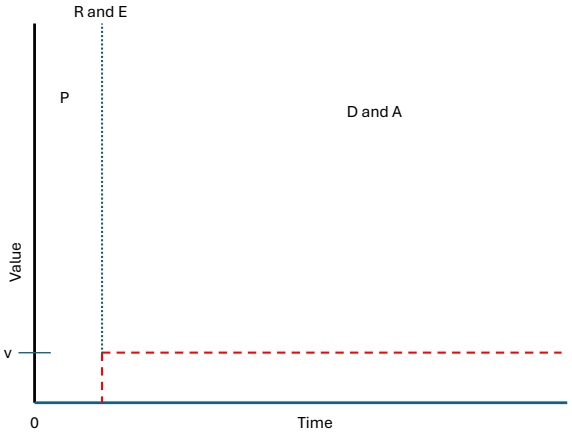

Fig. 1. Constant Information Value

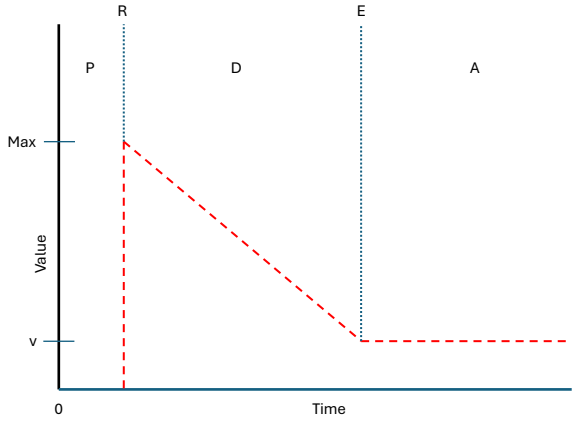

Fig. 2. Linear Value Drop

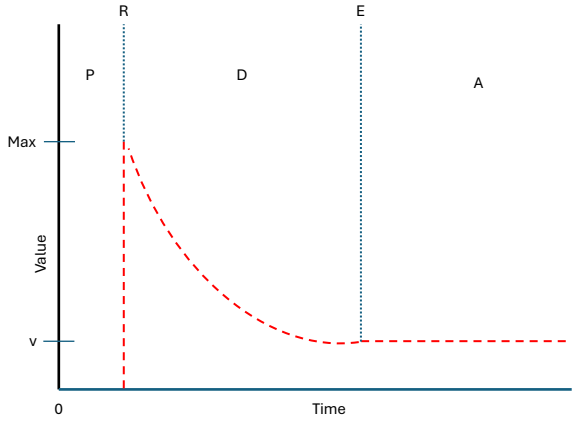

Fig. 3. Exponential Value Drop

clue to the need for the level of protection is the value of the end product that requires the data. However, once publicly revealed, there is no secret to be kept. This means before publicly disclosing the information, $|K| = \infty$, or as large as possible for encryption. Examples of such information are mathematical constants, such as π, the radar cross-section area of an aircraft, mathematical formulae, universal constants, and optimal algorithms.

C. Linear Drop

Some information loses value at a given linear rate over time. When the information is discovered, the value of the information falls at a fairly uniform rate right after the Rise (R) event until it reaches its asymptotic value. There may be noise imposed on the decay function, but on average, the decay will follow the linear decay proscribed by the formula

$$y = mx + b \tag{2}$$

over time, the decay is active. Applying the event, the math for the discovery, event, and decay allows for the description of information as

$$v(x) = \begin{cases} v_0 & \text{if } x < e_0 \\ \frac{v_0(x-e_0)}{e-e_0} & \text{if } x \geq e_0 \text{ and } x < e \\ v_{min} & \text{if } x \geq e \end{cases} \tag{3}$$

where e_0 is the time the event occurs. The loss of value is regular and even from the onset of the event. An example of such information comes from frequent weather events. A supplier, having advanced knowledge of an extreme weather event, such as a hurricane, could purchase essential supplies without artificially pushing the price up for those goods. When the event became general knowledge, the supply on hand would allow the supplier to make a significant profit. Premature disclosure would harm the supplier by raising the price, minimizing profit, or restricting the supply available to the store.

D. Exponential Drop

The mathematics of the exponential drop model has been well-studied in electrical engineering. This function naturally occurs in the form of time constants for resistive/capacitive (RC) circuits [15]. Of interest in this application is the decay portions of the function, which is mathematically described by the formula

$$v = v_0 e^{-\frac{x}{\tau}} \tag{4}$$

$$v_{90\%} - v_{10\%} = 2.2\tau \tag{5}$$

and is shown in Figure 3.

$$\tau = \frac{v_{90\%} - v_{10\%}}{2.2} \tag{6}$$

Exponential decay loses most of its values shortly after the information is found, and after a step initial drop, then slowly declines to its asymptotic value. Such a function means that most of the damage comes shortly after the discovery, and only a weak encryption function is needed to secure the information. Only incremental security is obtained using encryption

with a key space larger than the selected stop-gap loss. For the desired t of protection

$$t = \tau ln \frac{v}{v_0} \tag{7}$$

Examples of applications that follow this type of decay include having information for purchasing stock options [16]. Options are maximized if purchased well ahead of an event. The closer options are purchased to an event, the more the options cost and the lower the potential returns. The same effect occurs when a revolutionary technology is introduced. In many cases, the company that is first to market [17] with a revolutionary product can charge premium prices until the competition can catch up and introduce their versions of the product. The longer the secret is kept, the longer the company can reap the benefits of the higher pricing. Once the secret is revealed, competition begins to develop their versions, and consumers wait for the price drop due to competition.

E. Sudden Drop (Rectangular) Function

The final example of information value change is the "sudden drop" or rectangular module. Information that has a uniform high value as long as it remains a secret. Such information is vital to the planning and executing events to the advantage given to the person with that knowledge. Consider the advantage of a secret weapon or what Kerckhoffs [18] and Shannon [1] called "obscurity". Obscurity is a secret that, when it is revealed, loses much of its value. Some value may remain, but it is substantially reduced. That change is immediate upon discovery of the secret. There are several good examples of information that follows this model. They include a "zero-day" event [19], which consists of a never-before-seen attack methodology. Until the attack is analyzed and understood, no technique will stop the attack. Once understood, countermeasures are possible, and future attacks of that type can be prevented.

A second example is battle plans. Consider the example of D-Day [20]. The Germans did not know the date and location of the invasion. That secret was kept, in part, because the Allies set up fake armies and camps to confuse the Germans [21], [22]. The Germans knew that the attack was imminent. However, they did not know the exact date and location of the attack. The Germans could not respond effectively when the invasion occurred, and the invasion succeeded. Once the invasion started, the secret was out, and the information about the place and date/time no longer had as much value.

A third example is a trade secret. Companies can create and keep a competitive advantage by developing and protecting some essential formulas, processes, or practices. Once revealed and used by competitors, the value of the previously hidden information is significantly reduced.

Let t_{try} represent the time it takes to attempt to decrypt a message and determine if that decryption is correct. The term Δt is the length of time that a secret must be kept safe. Further, assume that n is an integer such that $n \geq 2$ that allows for a safety margin in a calculation. If the t me that the information

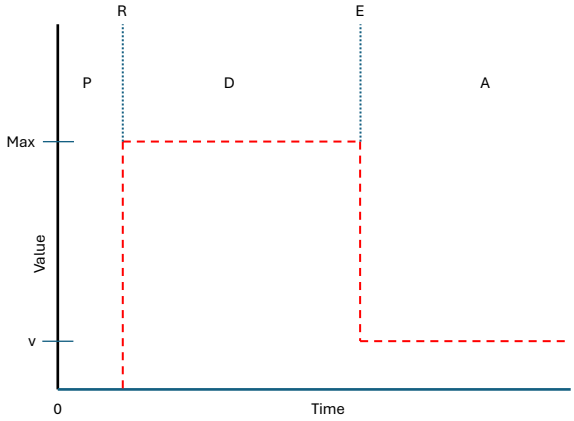

Fig. 4. Sudden Value Drop

Model	$\|K\|$
Constant Value	∞
Linear Drop	$\frac{n\delta t}{t_{try}}$
Exponential Drop	$t_{try}\tau ln\frac{v}{v_0}$
Sudden Drop	$\frac{n\delta t}{t_{try}}$

TABLE I
KEY SPACE SIZE BY MODEL TYPE

value is greater than the minimum value is represented by Δt and the time at which the encryption is applied is at time t where t lies within the bounds of Δ, then define $\delta t = \frac{t}{\Delta t}$. Then, the key space choice can be summarized in Table I.

F. Model Variance

The information does not have a uniform value for all users. Depending on a particular organization's business sector, business model, and market penetration, the information has a definite value assigned based on the potential damage or loss associated. For example, information about a car planned for introduction by one company has a different value to a food provider. Advances in quantum physics typically have little value outside of the physics, chemistry, and engineering fields. What follows from this observation and these examples is that the model of information value loss also varies for different people and groups.

The curves for information decay are smooth, representing the average and ideal response of the value of the information over time. As with most instantiations of an individual case, the noise will be imposed on the curve. That noise typically flattens the curve for short periods (see Figure 5). Drops in the value may also appear as sudden drops rather than smooth, continuous reductions in the value. However, on average, these variations are smoothed out, as shown in the figure. The cause of these differences is the circumstances surrounding the individual case being considered.

There are other causes for interrupting the smooth decline of the curve. For example, during the duration of the D phase of the curve, new uses for the information may be discovered.

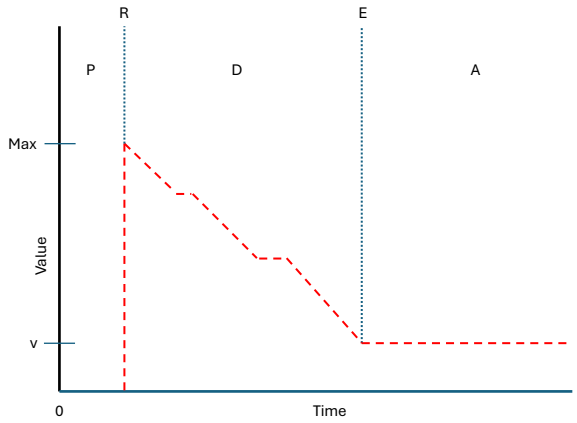

Fig. 5. Noise on Information Value Curve

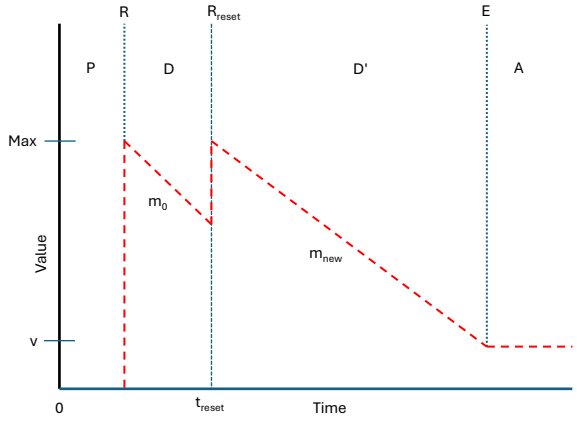

Fig. 6. Reset in Information Value

As a result of the discovery, the value of the information suddenly increases again. The discontinuity in the curve does not represent an exception to the monotonicity of the curve but rather represents a reset in the value due to the discovery of a new value, restarting the drop in value (see Figure 6. In this case, the value of τ_{new} or slope m_{new} for the new curve may not be the same as the τ_0 or slope m_0 for the old curve. The result is the need to reevaluate protected data and possibly re-encryption the previously encrypted data to accommodate the time reset of D' and the total protection period of $D + D'$. It is also possible that the curve and model for information value decay may be changed by events in the future of the curve due to new events. As a predictive tool, the curves approximate the fall in information value with sufficient granularity to select the correct cipher for protecting that information.

III. Applying Information Value to Security

A. Examples of Valuable Information

- Personal information - Some small number of pieces of seemingly trivial personal information are enough to uniquely identify an individual [23], [24]. In 2010, only 33 bits (of entropy) were enough to identify a person uniquely, and each bit has two possible values (0 and 1). Therefore, 2^{33} (equals to approximately 8.5 billion) is more significant than 6.6 billion (the estimated world population at that time) [25]. Considering each piece of personal information about a person as one bit, it will take at most 33 pieces of personal information to uniquely identify a person. This holds even now since the estimated world population in 2024 is 8.1 billion [26], [27]. Therefore, although personal information might seem trivial at first glance, premature revealing of each piece of information will narrow down the plausible individuals and aid in a person's unique identification. On the bright side, the lifetime of personal information is generally limited to the owner's life.
- Military Operations Orders - In the military arena, plans of action and their implementation are often of high value to adversaries. Suppose an adversary knows what friendly forces will be doing, mainly if this includes when those actions will be taken. They could then use that information to plan an effective counter-operation - whether that be an ambush, feint, deception, preemptive strike, etc. Operation orders [28] are written documents that contain the details of units and personnel involved in an attack, the time, place, and objectives of the attack, the chain of command to follow, communications details, and intelligence information about the enemy the attack is expected to encounter. The details in these documents can give an adversary significant advantages in an operation. However, once the operation begins, much of the value of that information is lost. However, few pieces of information, such as command structure or communications details, can stay constant or mostly unchanged across multiple operations.
- Insider information for new products - Resource suppliers can use this to set up a deal before anyone else has a chance
- Facts and formulae - Applications in all kinds of high-value fields. This includes math constants, such as π, e, and formulae, such as the quadratic equation and physics ballistics equations are examples of this class of information.
- Algorithms and procedures - Can lose value when improved upon or superseded.

B. Believability

A related problem to encryption arises from the study of networks and how users place confidence in the validity of the information. The issue of verifying the identity of the source of information online is longstanding and does not have an unambiguous solution. Users are left to determine the trustworthiness and identity of the information and its source. Once a deception is discovered and damage has occurred, the user has to decide whether or not to trust the source/data again, if trust is warranted, and when it should be granted.

Many attacks are run by hackers on websites and in attempts to "spoof" legitimate users [29] or steal identities [30]. Imme-

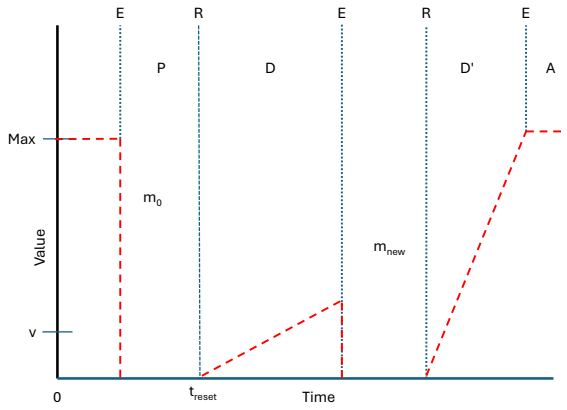

Fig. 7. Believability in Information Value

diately after discovering the deception, the user experiences a significant drop in trust (see Figure 7. Following the discovery, there is minimal or no trust in the source or information. This period can be arbitrarily long or infinitely long. After that period, the user begins to regain trust in the source or site. Given the previously introduced functions, arbitrarily denoted by $f(t)$, this relationship is

$$f_{rise}(t) = 1 - f(t) \tag{8}$$

After the event causing mistrust, the period of total mistrust is often followed by an increasing return of trust in the source or site. This can result from the user contacting the source and receiving an explanation of the event that caused the loss of trust. Trust again accumulates, sometimes based on the need for the information or the relationship between the user and source. With limited use, that confidence and trust may return until the source or site is fully trusted again. Multiple instances of attacks can cause this return of trust to rise and fall, as shown in Figure 7.

IV. Conclusion and Future Work

The declining value of information is vitally important in cybersecurity. Knowing how long a secret will cause problems if revealed allows the defender to select the proper cipher to keep that information safe. Different types of information and the conditions that exist for safeguarding the information contribute to that selection. Users must be able to match their use case to those previously identified or customize that calculation with newer, more appropriate/accurate models. There will also typically be noise on the curve from the environment, and there may even be a reset in the value of the information, including a change to the value model applied to the information.

Modeling information is also applicable to the problem of believability. This problem occurs when a website or identified user does something that can no longer be trusted. Such an action is often due to an attacker spoofing the user to prosecute a hack. The attacked person must then determine how long until their trust in that source or site can be restored. In this application, the same models can reflect the "distrust" in the source and the resulting renewal of trust in the site/source. Believability is not well studied and quantified at this time and requires future work.

This paper introduces four functional models for information reduction over time, along with examples of what types of information apply to the indicated type of value decay. However, these models are not the only models that may apply. As different problems are investigated and researched, additional models will likely be identified and reported on. These data models may be more complex and necessitate additional mathematical analysis. This information should be made publicly available for security personnel to use.

A database of ciphers and their appropriate key space figures should be kept and shared with security professionals. This data collection needs to be authoritative and peer-reviewed to ensure its correctness. The entries and analysis of the key space should be indexed for block size so that users can quickly and accurately calculate the value of the key space.

An accurate record of the computer's attack speed must also be made to calculate how many keys are needed to protect the secret appropriately as specified by the required key space. This information helps predict the time it takes for the value to decline. This database of key space needs to account for the true key space of the cipher, taking into account weak and equivalent keys, and any other heuristic attack that is effective on the cipher.

The capability of computers is constantly changing. Each change in computer hardware allows attackers to more quickly decrypt ciphers. Therefore, when the calculation is made to predict the future capabilities of newer computers, Moore's Law [31] needs to be applied. This law provides a bound for increasing hardware capability in operation. Moore's Law also provides an example of a time-varying function and a representative case of how hardware can affect information value, as well as demonstrating the methodology used to calculate the resulting changes in value. Hardware changes are an integral part of the calculation to predict the characteristic slopes of the model selected to describe the decay of information value. While the discussion about value has centered primarily on the effects of key spaces and hardware, more research is also required to identify what factors must be included for accuracy in setting the variables for each decay model.

References

[1] Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656 – 715, 1949.

[2] Thomas Cover and Joy Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc, New York, NY, 2nd edition, 2005.

[3] PALNI Consortium. Frame: Information has value - framework for information literacy for higher education - libguides at palni consortium, https://libguides.palni.edu/ilframework/informationvalue.

[4] Geoffrey Jehle and Philipp Reny. *Advanced Microeconomic Theory*. Prentice Hall, Englewood Cliffs, NJ, 2011.

[5] Peter Bernstein. *A Primer on Money, Banking and Gold*. John Wiley and Sons, Hoboken, NJ, 3^{rd} edition, 2008.

[6] Albert H Carlson, Benjamin Williams, and Sai Ranganath Mikkilineni. Is everlasting security necessary? In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*

(UEMCON) (IEEE UEMCON 2024), page 10, Yorktown Heights, USA, October 2024.

[7] Thomas C. W. Lin. Exutive trade secrets. *Notre Dame Law Reeviw*, 87(3), 2013.

[8] David Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 1996.

[9] John Kelley. *General Topology*. D. Van Nostrand Company, Princeton, 1955.

[10] Pamela Peterson Drake and Frank J. Fabozzi. *Foundations and Applications of the Time Value of Money*. John Wiley and Sons, Hoboken, NJ, 1^{st} edition.

[11] James M. Buchanan. *The World of Economics, Opportunity Cost*, pages 520 – 525. Palgrave Macmillan UK, London, UK, 1991.

[12] Uli Maurer. A universal test for random bit generators. *Journal of Cryptography*, 5(2):89–105, 1992.

[13] Steven W. Hawking. The information paradox for black holes. In *17th International Conference on General Relativity and Gravitation*, Dublin, Ireland, July 2004. see http://math.ucr.edu/home/baez/week207.html.

[14] M. R. Spiegal. *Schaum's Outline of Theory and Problems of Laplace Transforms*. McGraw-Hill Book Company, New York, NY, 1965.

[15] M.E. Van Valkenburg. *Network Analysis*. Networks series. Prentice-Hall, Englewood Cliffs, NJ, 1964.

[16] Sheldon Natenberg. *Option Volatility and Pricing: Advanced Trading Strategies and Techniques*. McGraw Hill, New York, NY, 2^{nd} edition, 2015.

[17] Fernando F. Suarez and Gianvito Lanzolla. The half-truth of first-mover advantage. *Harvard Business Review*, 2005.

[18] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5 – 83, 161 – 191, 1883.

[19] Lillian Ablon and Andy Bogart Rand Corporation. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Rand Corporation, 2017.

[20] Robin Neillands. *The Battle of Normandy, 1944*. Cassell, London, England, 2002.

[21] English Heritage. D-day deception: Operation fortitude south | english heritage, https://www.english-heritage.org.uk/visit/places/dover-castle/history-and-stories/d-day-deception, 2024.

[22] History. Fooling hitler: The elaborate ruse behind d-day | history, https://www.history.com/news/fooling-hitler-the-elaborate-ruse-behind-d-day, 2024.

[23] Federal Financial Institutions Examination Council. Authentication in an electronic banking environment, http://www.ffiec.gov/ffiecinfobase/resources/retail/ncu-01-cu_10_authentication_in_electronic_bank_envirn.pdf, 2001.

[24] Federal Financial Institutions Examination Council. Authentication in an internet banking environment guidance, http://www.ffiec.gov/pdf/authentication_guidance.pdf, 2001.

[25] The information that is needed to identify you: 33 bits. https://www.wsj.com/articles/BL-DGB-16975, Aug 2010.

[26] World population. https://en.wikipedia.org/w/index.php?title=World_population&oldid=1251270691, Oct 2024.

[27] Current world population. https://www.worldometers.info/world-population/.

[28] US Army. *FM 5-0 Planning and Orders Production*, 2022-11-04.

[29] K. Jindal, S. Dalal, and K. K. Sharma. Analyzing spoofing attacks in wireless networks. *2014 Fourth International Conference on Advanced Computing Communication Technologies*, page 398 – 402, 2014.

[30] John Brandon. Your online identity sells for exactly $1,170 on the dark web – here's how to block the sale, https://www.foxnews.com/tech/your-online-identity-sells-for-exactly-1170-on-the-dark-web-heres-how-to-block-the-sale, 2018.

[31] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8), 19 April, 1965.