MP 180676
MITRE PRODUCT

MITRE

ECHO Data Analysis

Project No.: 10AOH810-JF

Lexington Park, MD

Authors:

F. Lynam
F. DiBonaventuro
M. Mickelson
L. Oringer
S. Ricks

Peer Review

R. McInnes
M. McFarren

October 2019

Abstract

This paper outlines the mathematical basis for the predictive vulnerability rates produced by the ECHO model. An overall empirical equation for vulnerability discovery rate is presented and each piece of that equation is elaborated on in detail. The underlying theory for predicting vulnerability discovery rates and its basis in the literature are discussed, as well as sources of data used to develop the empirical formula and the particular appropriate application and scope of that data. In practice, much of the mathematical application of this function is automated by Trace tools, however, an understanding of this paper is an important aide to analysts intending to apply the ECHO model to a system under assessment. This paper argues that this rate function is expected to provide a reasonable yet conservative estimate of residual risk to system with no known vulnerabilities, however additional research is warranted to further improve this work.

Overview

This paper describes the derivation of a quantitative, data-driven empirical function to estimate the probability of success of executing any one state transition in the ECHO (Estimated Cyber Hardness by Observation) traversal model as a function of time invested and the underlying technology. Use of this function within an appropriate analytical framework, such as Trace (Traversal-driven Risk Assessment of Composite Effects) will allow for an evidence-based approach to estimating cyber risk. Future work will reduce the uncertainty in the final estimated values.

The purpose of the ECHO traversal model is to provide a universal structure which captures within it all possible permutations of cyber weapon design. The probability of any one state transition in the ECHO traversal model is critical to understanding the probability of successful cyber weapon deployment. Here, those individual state transition probabilities are provided as a function of adversary resources ("time, talent and treasure") and the technologies involved in the weapon attack path (code complexity, age and functionality). The fundamental equation derived in this research can be summarized as follows:

$$P_{Exploitation} = 1 - e^{-R_{Successful\ Exploitation} t[days]}$$

Equation 1

$$R_{Successful\ Exploitation} = S_{Design\ Exploitability} * R_{Vulnerability\ Discovery} * F_{Vulnerability\ Applicability} * I_{Technology\ Facilitation} * L_{Sufficient\ Investment}$$

Equation 2

Where the rate of successful exploitation is a function of the design of the system and the investment of the adversary. In application, the exploitability of the design must be determined (with a coefficient of either 0 or 1) based on the applicability of the threat concept from the ECHO traversal model. For example, you can't exploit what isn't there. If a system relies on no data from the network, then threat concepts from the ECHO model such as "Resource Manipulation" simply do not exist, resulting in a design exploitability of 0.

Next, the adversary must both discover a vulnerability as well as have the vulnerability apply to the threat concept in question. This is captured by a base rate of vulnerability discovery by high capability organizations, which is reduced to some partial fractional rate based on how often specific types of threat concepts apply to discovered vulnerabilities. For example, vulnerabilities might be found every day, but only every fifth one might actually be useful for a specific attack.

Then, the underlying technology plays a role in the rate of vulnerability discovery, and the function must control for less ubiquitous or more embedded technologies, which naturally exhibit a lower vulnerability discovery rate. It's harder to find and exploit flaws in the design of special-purpose systems, like programmable logic controllers or global position system receivers, and that reality is observable in reference data.

Lastly, the level of adversary investment influences the rate of vulnerability discovery, where the rate of successful exploitation has been observed to have a theoretical ceiling limit. This can be very difficult to empirically measure, but as the rest of the function is built around the most capable adversaries, reductions to analyze for less capable adversaries should not be necessary for most applications.

Probability of Exploitation

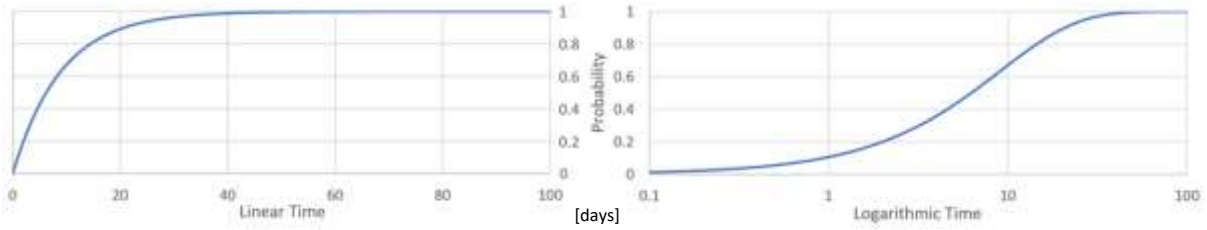
Equation 1 uses an exponential distribution to estimate the mean time to discovery of a novel vulnerability.[1] It has been argued that this is representative of a Poisson process model for the accumulation of vulnerabilities over time.[2] In a Poisson process, events happen randomly, but over a long period of time they average out to a particular number of events per time period; an event rate. It can be shown that using a Poisson model for accumulation of events is equivalent to using an exponential model for the time to the next event, where the probability of n events to occur within interval t given a mean event rate of r has a general form, and the probability for at least one threat event to occur in t is given by:

$$P(n;t) = \frac{r^n}{n!}e^{-rt} \rightarrow P(n>0;t) = 1 - P(0;t) = 1 - \frac{(rt)^0}{0!}e^{-rt} = 1 - e^{-rt}$$

Equation 3

This Poisson distribution is now a simple exponential probability distribution, and is completely described in time by the rate constant (r). For ECHO, the value $R_{Successful\ Exploitation}$ is derived from an understanding of the context of the specific cyber threat events involved in an attack and how that relates to the adversary's level of effort to execute an effect. That adversary work factor is determined by comparing the system context of each of the specific steps in a given attack path against the rate of discovery for similar vulnerabilities in several reference data sources. The result is a probability function that describes the odds of an adversary successfully weaponizing an attack path.

Trace, Traversal-driven Risk Assessment of Composite Effects, is a stochastic adversarial process analysis which uses the ECHO function to assess cyber effects. Trace combines all these steps and all possible paths into a cumulative distribution function of the probability of a successful attack as a function of time invested. The resultant curve generally takes the shape shown in the below figure. Characteristics of a system which vary the adversary work factor will vary the slope of this curve consistent with expert intuition. For example, higher capability adversaries are more likely to be successful in a given amount of time, and more common vulnerabilities are more likely to be discovered and exploited.



Design Exploitability

The ECHO function provides a method to estimate the mean time between discovery of novel vulnerabilities. Here, those vulnerabilities are characterized in terms of the threat concepts in the ECHO

[1] E. Rescorla, "Is Finding Security Holes a Good Idea?" IEEE Security & Privacy, January-February 2005

[2] M. McQueen, W. Boyer, M. Flynn, G. Beitel, "Time-To-Compromise Model For Cyber Risk Reduction Estimation," Quality of Protection Workshop, ESORICS, Idaho National Laboratory, September 2005

function traversal model which require exploitation of pre-existing system design flaws. These threat concepts include:

#	Threat Concept	Brief Description
1	Abuse of Native Code	Use intentional design features to inject code
2	Abuse of Pivot Functions	Use intentional design features to pivot
3	Authentication Implementation Flaw	Exploit a design flaw in how a system manages authentication to bypass the need for credentials
5	Denial of Local Services	Disrupt the internal resources, but not the network
6	Denial of Network Services	Disrupt the network, but not the internal resources
7	Exploitation of Poor Memory Management	Exploit programming errors to change system memory
9	Indicator / Alert Manipulation	Falsify indications via local malicious code
10	Injecting Faults	Falsify network traffic to induce a predictable response not intended to be there
12	Interface Overload	Input data an interface is designed to handle, but that it handles in an unexpected manner
15	Privilege Management Implementation Flaw	Exploit a design flaw in how a system manages privileges to escalate to kernel mode
16	Resource Manipulation	Falsify network traffic to induce a predictable, programmed response

The analysis framework included with the traversal model itself provides the means to determine whether the design is fundamentally exploitable:

$$S_{Design\ Exploitabilty} = 0\ or\ 1$$

Equation 4

Fundamental Relations of Source Data

The ability to make estimates of the time required to discover novel vulnerabilities for these threat concepts requires representative data and a credible causal relationship. These fundamentals support future hypothesis testing and model evolution as more data becomes available.

Design of Conservative, Bounding Analysis

Due to a lack of existing rigorous practices available to describe the exhaustive space of cyber effects, there are often many unknowns in cyber analysis. This model attempts to produce a simple first-step, resulting in the need for simplifying assumptions where further details may be highly context-specific or relevant data is otherwise unavailable. Such assumptions can produce an error or bias between the predicted result and reality.

Any error which may potentially result in ignoring a risk effectively forces the recipient of the analysis to accept that risk unwittingly. To avoid this, the analysis must err conservatively, ensuring that wherever an unknown effect exists, that unknown is assumed to be a risk and accounted for accordingly. Another way to manage unknown error is to use bounding cases and assume the worst case chain of events as a baseline.

This results in conservative errors that ensure no risks are understated, but may also result in an inability to prove an analysis shows acceptably low residual risk. Where the cost of actions needed to mitigate an over-conservative risk are high, bounding assumptions within the model can be reassessed, "sharpening the pencil" and potentially buying back margin not by changing the system, but by reducing the known conservative bias and error in the conclusions.

Data Sources

The ECHO function derives its key parameters from disparate data sources. Of the five parameters in equation 1, the four quantitative values are derived from observable evidence in order to ensure that the resultant probability estimates are well bounded by real data. While some opportunity to leverage subject matter expertise to fine-tune analysis is provided, that subjectivity is strictly limited to within bounds which are clearly defined on either end by observed data. Cyber effects are poorly understood, particularly in rigorous and consistent engineering terms, are often poorly documented in multiple, overlapping databases and are often considered highly sensitive. Consequently, reliable and consistently collected or structured data is challenging to acquire in this domain. The sources for all of the data use here were carefully selected to find references that provided reasonable controls against confounding effects. No one data source exists that would be suitable to characterize all of the dimensions of this problem.

For $R_{Vulnerability\ Discovery}$, an existing analysis of vulnerability discovery rates was used. Use of a large-scale repository of known vulnerabilities would be unsuitable for this factor due to the confounding influences involved in how vulnerabilities are added to large-scale repositories. For example, software with a larger install base or software with a tighter feature update cycle would be expected to have a higher rate of vulnerabilities incorporated into a large-scale repository. However, while those influences change the rate at which vulnerabilities are discovered by the general public, they are not relevant to the rate at which vulnerabilities would be discovered by a dedicated adversary. The data source selected for this factor provides better controls for vulnerability discovery by a dedicated, isolated team focusing on a specific technology.

For $F_{Vulnerability\ Applicability}$, a large-scale vulnerability repository was selected, specifically the Common Vulnerabilities and Exposures (CVE) repository. This factor is actually a distribution of relative rates of vulnerability discovery across categories of vulnerabilities. This distribution has been informally observed to hold fairly consistent across vulnerability types over time for the large-scale repository. However, specific technologies might have different distributions. Without significant additional research it would be difficult to fully characterize whether or how this distribution might change with the specific technology in question. Consequently, it is desirable to control the source data for this factor by sampling across as wide a variety of technologies as possible in order to support a mean distribution that typifies the phenomena. Large-scale vulnerability repositories provide the best available depth of data to meet this need. However, if this distribution does vary by technology, the derived distribution here would be expected to skew toward commercial applications with a large install base.

For $I_{Technology\ Facilitation}$, the Department of Homeland Security Industrial Control System Cyber Emergency Response Team (DHS ICS CERT) incident report data was selected. The DHS ICS CERT particularly focused on providing emergency response to explicitly heterogenous facilities which contain a mix of traditional business systems and special-purpose industrial control systems. Consequently, DHS

ICS CERT incident response data is expected to provide an effectively random sampling of incidents out of a population that is approximately equal parts business systems and control systems. This allows the DHS ICS CERT data to be considered as roughly controlling for the size of the install base of these two categories of systems, allowing for incident rate to provide an approximation of vulnerability discovery rate. A large-scale vulnerability repository would naturally be unsuitable for deriving this factor due to the compounding influences of size of install base and public interest in vulnerability discovery, two influences that are minimized by use of the DHS ICS CERT data for this purpose.

For $L_{Sufficient\ Investment}$, general observations from subject matter expertise as documented in an existing threat assessment model were leveraged.[3] As this factor is only used to estimate discovery rates at investments below the Tier VI adversary level, an analysis not normally performed, additional controls on the data source for this factor were not considered. Further, no alternative reference data was readily available. This factor is included primarily to ensure the ECHO function is able to provide estimates that can scale consistently with existing understandings of adversarial threat capability levels if so desired by an analyst.

Events, Vulnerabilities, Exploits and Incidents

Any cyber effect will take some amount of time and resources to discover, develop and implement. In particular, the mean rate of vulnerability discovery in major software platforms with extensive analysis and test teams is approximately one critical vulnerability per month (30.42 days).[4] This places an upper limit on the maximum mean rate of vulnerability discovery by a dedicated, well-resourced team working on common, commercially available software. In the overall ECHO function, this is used for the probability that a vulnerability is discovered as a function of time :

$$R_{Vulnerability\ Discovery} = \frac{1}{30.42[days]}$$

Equation 5

For any one effect discovered at a given fixed resource level, this amount of time can therefore be treated as a mean rate in a Poisson process. A successful execution of a cyber effect requires only a single event to occur in the Poisson discovery process, resulting in a simple exponential distribution in time.

While the peak rate could be conservatively applied to all vulnerabilities of any kind in all systems, such a treatment would be dramatically overconservative. Vulnerability discovery rate will draw down based on circumstances related to the type of vulnerability needed by the adversary, the underlying technology being examined and the available resourcing.

Extensive and highly reliable data on different families of cyber vulnerabilities across a wide variety of technologies is not readily available. However, extensive data does exist on vulnerabilities, exploits and

[3] J. Burtch, C. Goodrich, M. Whitmore, T. Schonfeld, et al, “Cyber Threat Model Analysis for Acquisition Program(s),” Johns Hopkins University Applied Physics Laboratory, Prepared for the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

[4] M. McQueen, W. Boyer, M. Flynn, G. Beitel, “Time-To-Compromise Model For Cyber Risk Reduction Estimation,” Quality of Protection Workshop, ESORICS, Idaho National Laboratory, September 2005

incidents across different groups of technologies and industries. This data can be used to make assertions about event rates given appropriately bounding constraints on the applicability of the data used and predictions made.

Anecdotally consistent with the above observation in commercial software vulnerability discovery, documentation of a cyber defensive operation engaging an active attack from APT 29 (aka The Dukes, Cozy Bear), a notional Tier VI adversary generally assumed to be affiliated with the Russian government notes direct observation of three updates to the SeaDaddy malware kit delivered in real-time during the approximately 100-day attack.[5] Reasonably assuming these updates were intended to exploit new software vulnerabilities not exploited in previous iterations of the SeaDaddy malware kit, this represents an observed Tier VI event rate near the above noted potential maximum of one unique threat event per month. Further adversary interaction events could be assessed to improve the confidence in this figure on a per-adversary basis given appropriate data.

Vulnerability Type Distribution Invariance

Vulnerabilities from the Common Vulnerability Enumeration (CVE) database were randomly sampled and mapped to threat concepts from the Trace threat concept catalog. The discovery rates of the sampled vulnerabilities are assumed to have a distribution consistent with the overall discovery rate: a constant Poisson arrival process. By observation, this treatment appears consistent with the distribution of vulnerabilities types over time.

96 vulnerabilities in the CVE database were evaluated for applicability to the threat concepts in question. Individual CVE entries often represent multiple threat concepts, depending on the context of the system under assessment. Consequently, 181 threat concept observations were made across the 96 sampled CVE entries, distributed as follows:[6]

ID	**Threat Concept**	**CVEs**
1	Abuse of Native Code	27
2	Abuse of Pivot Functions	7
3	Authentication Implementation Flaw	22
5	Denial of Local Services	26
6	Denial of Network Services	13
7	Exploitation of Poor Memory Management	11
9	Indicator / Alert Manipulation	8
10	Injecting Faults	16
12	Interface Overload	23
15	Privilege Management Implementation Flaw	19
16	Resource Manipulation	9

Based on the above discussion, the probability that a given vulnerability will align to a particular threat concept can be treated as the fraction of the number of CVE entries applicable to that threat concept

[5] M. Dunwoody, N. Carr, “No Easy Breach,” Mandiant, DerbyCon 2016

[6] Note that not all threat concepts require the existence of a pre-existing flaw of this nature, some are a simple result of the design of the system. Threat concepts requiring no pre-existing flaw are not shown in this table.

out of all CVEs sampled. Based on the sample size provided here, this value has a confidence of 95% at an error of 10%:

$$F_{Vulnerability\ Applicability} = \frac{CVE\ entries\ applicable\ to\ threat\ concept}{CVE\ entries\ sampled}$$

Equation 6

Additionally, it was observed that, consistent with the discussion in the traversal model, CVE entries which bridged multiple threat concepts fell into three general varieties: misuse of intended functionality, exploitation of unintended functionality and authentication implementation flaws. Two to five threat concepts were often found to apply to each of these.

Threat concepts 1, 2, 5, 6, 9, 12 and 16 often occurred in small groups associated with individual CVE entries vulnerable to misuse of intended functionality. Threat concepts 5, 7, 10, 12 and 16 often occurred in small clusters for CVE entries related to exploiting unintended functions. Threat concepts 3, 6, 15 and 16 often applied for authentication implementation flaws. These observations suggest a related model of the nature of vulnerability may exist prompting the consistency of these empirically-observable relationships.

Also of note, threat concepts in the traversal model have been generalized to facilitate mapping of common vulnerability themes into specialized technologies that have little or no observed vulnerability data. Consistent characterization of the threat concepts in this manner allows estimating threat concept-specific rates that may be higher than the real discovery rate in the under-observed technology but still lower than the overall rate defined in equation 5.

It is important to recognize that this simplifying assumption may be non-conservative, as vulnerability distribution could potentially vary by technology. The only clear means to bound that risk at this time would be to assume that all vulnerability types are discovered at the peak rate, which would be overly-conservative. This potentially non-conservative error is considered reasonable by the authors pending further available data.

Vulnerability Rate, Exploit Rate and Incident Rate

While vulnerability discovery rate data for common, commercially available software puts an upper limit on adversarial activity, a comparable data source is not readily available for specialized or embedded systems, which lack sufficient install base to justify comparable levels of dedicated vulnerability analysis experts in the public sector.

Large-scale vulnerabilities data sources, such as CVE, have an inconsistent treatment of specialized technologies, such as industrial control, supervisory control and data acquisition and other cyber physical systems. Historically it has been unclear if CVE is the correct repository for this data, and investigation of vulnerabilities by the general public has been less widespread. Consequently, there is a reasonable concern that these sources are an unreliable reference for the impact of underlying technology on vulnerability discovery rate.

However, a high capability adversary may invest as much expertise as necessary in such technologies to meet the potential peak rate, even if the public sector does not, resulting in a need to extrapolate between commodity systems and specialized systems via some other data source. Cyber incident rates are used for this extrapolation based on the following discussion about their appropriateness.

Cyber incidents are not directly observed at the mean rate for several reasons. Primarily, not all intrusions are observed, meaning the number of observed incidents is less than the number of actual incidents. Further, not all incidents are unique events due to exploit and technology reuse. Often, multiple incidents represent common exploits on common technology simply observed at different facilities. The occurrence of such "redundant incidents" is poorly controlled for in reference data. Additionally, inherent operations security considerations with higher capability adversaries further obscure the relationship between exploit development and observed incidents.

Consequently, there is no clear mechanism to manage the relationship between the rate of observed incidents and the rate of vulnerability discovery. Incident data can only be reasonably used for assessing factors independent of these issues, such as the effect of underlying technologies. Herein, incident report data is used as a basis for scaling weapon development rate by underlying technology, where adversary cross section and threat concept distribution are treated as invariant across technologies.

Several options are available to address the relationship between incident rate and technology. Notionally, incident data could be controlled for source vulnerability or threat concept vice total number of incidents across a technology, but this level of data analysis, while potentially viable, would require a level of effort beyond the scope of the current analysis. However, due to lack of available detailed incident data, redundant incidents are treated here as constant regardless of influencing factors such as threat concept, underlying technology or adversary resourcing. However, this non-conservatively treats uncommon technologies as having the same redundant incident rate as common technologies, which would be challenging to justify considering the observable greater diversity of technologies, naturally precluding as extensive of reuse. Additional data is needed to better characterize this space.

Technology Influence

This treatment of incident data thus allows for some measure of how the technology itself influences the rate of vulnerability discovery. DHS ICS CERT incident response meta-data (provided by ICS CERT for the purpose of this specific analysis) was reviewed across CERT responses closed from 2013 to 2016, inclusively. This data indicated only about half as many observed incidents for technologies considered "industrial control systems" by DHS ICS CERT (93 events categorized as "ICS" or levels 4-6) relative to "corporate" systems (206 events categorized as "Corporate" or levels 1-3). A further 658 incidents were not sufficiently categorized in the metadata to be used for this assessment. Rate differences within the groups (between 1, 2 and 3, for example) was not meaningful at the available sample size to make reliable inferences.

Where the particular asset or technology under assessment aligns with systems characterized by ICS CERT as industrial control, embedded and safety critical systems, a vulnerability discovery rate reduction factor of 2.2 is applied consistent with the rate reduction observed in the reference data:

$$I_{Technology\ Facilitation} = \frac{1}{1\ or\ 2.2\ if\ control\ system}$$

Equation 7

This factor represents the best data-driven estimate available and is valuable for rapid, empirically-based triage. However, this value lacks the fidelity desired for trade space analysis or considered attainable by Trace subject matter experts. In lieu of this explicit figure, a Trace custom tailored catalog informed by subject matter expertise across a wide variety of technologies is available to provide expert

tailoring of the technology facilitation factor. Direct comparisons between specific technologies at a scale not attainable with empirically-based methods is provided on a per-component and per-threat concept level, built around this value as a reference scale. Further data collection in this area can provide a more quantitative basis for these currently subjective figures.

Vulnerability to Exploit Conversion Rate

In available public data, not all vulnerabilities become exploits. In particular, long-lived and more exploitable vulnerabilities more often have observed exploits, and in general the number of vulnerabilities is greater than the number of exploits. However, more than one exploit has been observed for some vulnerabilities. Thus, mathematically defining the relationship between vulnerability discovery rate and exploit observation is challenging. .

Nevertheless, a high capability adversary could have a better vulnerability to exploit conversion rate than the general population, with a conservative ceiling of 100%. No data is currently available on high-tier adversary conversion rates to justify reduced conservatism.

Some vulnerabilities in CVE have multiple documented exploits. For the purpose of ECHO models, two exploits for a specific vulnerability on a specific asset is expected to add little additional value to an adversary, and consequently the vulnerability-to-exploit conversion rate is treated as no higher than 100%. This supports the simplification of the Poisson distribution into an exponential function, and relates significantly to adversary decision making policy. An instance where an adversary is trying not to "burn" exploits during covert peacetime operations could warrant a different treatment of this area, but is not addressed here.

Notably, real weaponization of a vulnerability requires a non-zero development time and can be handled several different ways. All vulnerabilities could take an equal time to weaponize regardless of any other factors, or alternatively, vulnerabilities could take time in proportion to vulnerability discovery rate, more consistent with the concept of adversary work factor.

However, as one exploit's weaponization resourcing may not interfere with discovery resourcing or another exploit's weaponization, the overall discovery rate should not be limited by weaponization. Thus, the weaponization breakout time would be a constant phase offset whose rate would be primarily limited by the initial vulnerability discovery rate. Therefore, while individual exploit development time (weaponization) may even be greater than individual vulnerability discovery time, there should be no impact to time between subsequent weaponizations. This allows for the conservative simplifying assumption that weaponization rate is equal to discovery rate.

Adversary Investment

All data up to this point has been presented to address an Tier VI, peer or near-peer, cyber adversary capability. This level is considered by the analysts to be appropriate for use in any analysis supporting national security cyber defense objectives. However, some understanding of how adversary capability relates to overall risk may be of value for special cases. While the supporting data which describes the shape of the curve for this factor does not warrant extensive use of this function for capability-specific analysis, this factor is included in the ECHO function for completeness as a reference method to capture the impact of adversary capability level.

A curve was described to fit between the $R_{Vulnerability\ Discovery}$ value for high-tier adversaries and the observations of actual event rates in DHS ICS CERT data for low-tier adversaries.[7] An existing model for a rough quantitative capability measure between high-tier adversaries was used to characterize the intermediate shape of the curve, based on the observation that a Tier VI adversary can "evade detection" for 1 month, a Tier V adversary for 1 week and a Tier IV adversary for 1 day.[8]

These figures provide a quantitative means to characterize adversary capability highly consistent with the model presented by the ECHO function. By this reference, a Tier VI adversary would notionally weaponize novel vulnerabilities at a rate 30x faster than a Tier IV, and a Tier V is likewise notionally 7x faster than a Tier IV. An exponential fit (consistent with observations in the supporting analysis for equation 5) between the observed high-capability rate and the low-capability data, fits roughly along the curve described by these quantitative relative rate factors, and provides an approximation of the variation of composite threat event rates with changes in adversary tier.

In implementation, this function produces the fraction a given adversary is expected to operate at relative to the overall rate of a Tier VI adversary, producing approximately 1 at the Tier VI level. Consequently, it only needs to be used in analyses focused on estimating risk to capabilities below the Tier VI level:

$$L_{Sufficient\ Investment} = 0.0002e^{0.041*adversary\ tier^2+1.1735*adversary\ tier}$$

Equation 8

[7] "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report," National Cybersecurity and Communications Integration Center / Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security, 2016

[8] J. Burtch, C. Goodrich, M. Whitmore, T. Schonfeld, et al, "Cyber Threat Model Analysis for Acquisition Program(s)," Johns Hopkins University Applied Physics Laboratory, Prepared for the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

The ECHO Function

These analyses produce a data-derived empirical function which places an upper limit on the mean probability of a particular cyber weapon effect. When used in conjunction with Trace , the result is a maximum limit to the mean probability of mission compromise through cyber effects. Essentially, this method provides a means to make a statement with reasonable certainty that expected risk is no higher than the computed value:

$$P_{Exploitation} = 1 - e^{-R_{Successful\ Exploitation} t[days]}$$

Equation 1

Where:

$$R_{Successful\ Exploitation} = S_{Design\ Exploitability} * R_{Vulnerability\ Discovery} * F_{Vulnerability\ Applicability} * I_{Technology\ Facilitation} * L_{Sufficient\ Investment}$$

Equation 2

Thus:

$$P_{Exploitation} = 1 - e^{\left[-\{0\ or\ 1\ if\ design\ is\ susceptible\} * \left\{\frac{1}{30.42[days]}\ maximum\ rate\right\} * \left\{\frac{CVE\ entries\ applicable\ to\ threat\ concept}{CVE\ entries\ sampled}\right\} * \left\{\frac{1}{1\ or\ 2.2\ if\ control\ system}\right\} * \left\{0.0002e^{0.041 * adversary\ tier^2 + 1.1735 * adversary\ tier}\right\} * t\right]}$$

Equation 9

Conclusion

The ECHO function attempts to accounts for the systemic elements considered to dominate the rate of vulnerability discovery, as reflected in the available data. However, it is recognized that this approach to this field of study is relatively nascent and this function may fail to account for additional relevant factors, even ones available in data already used here. Nevertheless, the formulation presented here is considered reasonable and conservative, and when used with the proper application of the ECHO model is expected to afford a bounding representation of adversarial threat vector decision space when attacking a cyber system. Future research can and should be pursued to improve, expand and refine this basic formula as the community's understanding of this problem space evolves over time.

Appendix A – Uncertainty

This appendix discusses sources of accountable error in the available data.

S, Design Exploitability

Design exploitability is a purely objective factor, determined based solely on the presence or absence or design factors. This is a potential source of systematic error, which is not accounted for here.

R, Vulnerability Discovery

The standard rate of vulnerability discovery was taken from McQueen, 30.42, who cites Rescorla's p<0.05 curve. Presumably, this is the theta for the bias-checked curve, which is not included in the Rescorla paper. The 95% confidence bound corresponds to 1.96 standard deviations from the mean on a normal distribution (McQueen posits this is a Poisson process, whose mean would then be normally distributed). No standard error is available for the Rescorla bias-checked data set, but there is a standard error available for a specific year with a low p value. That is 1.92. This results in an error of +/- 3.8 days at a 95% confidence, or 12.5%.

F, Vulnerability Applicability

This factor was computed by the team and has a 10% error at the 95% confidence interval.

I, Technology Facilitation

This data set focused on categorization and determination of relative proportions. Consequently, it contained 299 events categorized as either an IT system (206 systems with a value of 0 here) or CPS system (93 systems with a value of 1 here). This results in a mean value of 0.311 across the data set. The standard error can be computed as follows:

$$\sigma = \frac{1}{N-1}\sum(x-\mu)^2 = 0.215$$

$$\sigma_\mu = \frac{\sigma}{\sqrt{N}} = 0.0124$$

The 95% confidence, assuming a normal distribution, results in a z value of 1.96 and an uncertainty of +/- 0.0244 for this coefficient, or 5.4%.

L, Sufficient Investment

This factor has insufficient empirical basis to determine uncertainty. By design, when a Tier 6 adversary is assumed, this factor is 1 and introduces no uncertainty.

Overall Uncertainty

As these are multiplicative factors, the uncertainties combine using the root sum of squares of the relative uncertainties to produce the 95% confidence interval on the estimated discovery rate:

$$u_{total} = \sqrt{u_R^2 + u_F^2 + u_I^2} = 16.7\%$$