No Free Lunch in Cyber Security

George Cybenko
Thayer School of Engineering, Dartmouth College
Hanover NH 03755 USA
gvc@dartmouth.edu

Jeff Hughes
Tenet3
Dayton, Ohio USA
jeff.hughes@tenet3.com

ABSTRACT

Confidentiality, integrity and availability (CIA) are traditionally considered to be the three core goals of cyber security. By developing probabilistic models of these security goals we show that:

- the CIA goals are actually specific operating points in a continuum of possible mission security requirements;
- component diversity, including certain types of Moving Target Defenses, versus component hardening as security strategies can be quantitatively evaluated;
- approaches for diversity can be formalized into a rigorous taxonomy.

Such considerations are particularly relevant for so-called Moving Target Defense (MTD) approaches that seek to adapt or randomize computer resources in a way to delay or defeat attackers. In particular, we explore tradeoffs between confidentiality and availability in such systems that suggest improvements in one may come at the expense of the other. In other words, there is "No Free Lunch" in cyber security.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Unauthorized access

Keywords

Security metrics; formal models; confidentiality; integrity; availability; diversity; moving targets

1. INTRODUCTION

This paper develops a quantitative framework for modeling diversity and showing how diversity can affect the cyber security goals of systems and missions, including confidentiality, integrity and availability (CIA) individually as special cases. We develop probabilistic models for diversity and each of the CIA goals using the *time-to-compromise* random variable for when a component is successfully attacked. This allows us to demonstrate that there are quantitative and intuitively clear consequences of diversity when defending the CIA goals against both single and multiple attackers.

In particular, it is shown how the probabilistic security properties of components relate to the security properties of systems built out of those components. As such, we hope to develop the beginnings of a cyber security analog of reliability engineering.

A major contribution of this paper is that it offers quantitative bounds on employing diversity. We show that certain types of diversity may offer no added security benefits when the systems are being attacked by multiple adversaries. These results illustrate a promising approach for monoculture versus diversity cost/benefit trade space analyses.

1.1 Previous Work

Previous discussions about monoculture and diversity in the context of information assurance and cyber security can be found in [12, 3, 16, 8, 20]. That body of work is largely qualititative rather than quantitative, appealing in essence to intuitions and similarities with biological diversity.

Mathematical aspects of diversity and especially natural limits to diversity have been studied in the mathematical biology literature [11, 10, 1]. That work addressed the important question of how much diversity can exist in the limit, when the resource types in an environment are constrained. At this time, we are not aware of corresponding analyses of computing systems' diversity from the point of view of how much diversity is sustainable in a particular computational ecosystem.

1.2 Organization of the paper

After this introduction, we introduce and review some of our underlying concepts in Section 2. Section 3 contains the main results concerning quantification of diversity in the context of the CIA security goals. Section 4 is a summary of results together with ideas for future work. The Appendix contains additional details of derivations of the results summarized in Section 3.

2. BACKGROUND CONCEPTS

2.1 Confidentiality, Integrity and Availability Security Goals

Our basic model is a network of n nodes that comprise an asynchronous distributed system. These nodes could be

MTD'14, November 3, 2014, Scottsdale, Arizona, USA.

http://dx.doi.org/10.1145/2663474.2663475.

mirrored web or database servers, clients, routers or other replicated devices or services in an information system. The designer has a choice of making the n nodes the same (homogeneous, monoculture) or making the n nodes different (that is, diverse, moving targets, heterogeneous) in some way.

A *compromise* of a node (component or device) means that an attacker has control of that node such as root or administrator privileges in an operating system for example. The goals of a compromise are often summarized as one of confidentiality, integrity and availability [18]. We interpret these goals in the context of a networked system of n redundant components.

In this paper, *availability* means that at least one of the n nodes has not been compromised and is therefore functioning properly. Stated otherwise, not all of the nodes in the system have been compromised and so at least one is still functioning in a reliability theory sense.

By *confidentiality*, we mean that none of the nodes have been compromised. This definition is based on the assumption that all clients, servers or other nodes under consideration contain or have access to critical, possibly the same, information. Therefore if one node is compromised that crtical information is available to the attacker and so confidentiality of the overall system has been breached.

By *integrity*, we mean that a majority of the nodes (components) have not been compromised so that if we request information from the n components and compare results, at least $n/2$ of the results will match. Once at attacker has compromised more than $n/2$ of the components, we no longer have any confidence that the information being provided by a majority is correct. Byzantine failures [9] can also be modeled in this framework whereby at least $n/3$, a different but constant fraction, of the components need to be compromised for an integrity attack.

Finally, we point out a principle assumption of this work. The "value" of the system for a user proceeds from availability through integrity to confidentiality. If a system's availability is completely denied (for instance in a successful distributed denial of service attack) discussions of time-to-compromise are moot in the context of our current analysis.

2.2 The Time-to-Compromise Random Variable

The *time-to-compromise*, t_i, of the ith node is a random variable distributed according to a probability density function, $f_i(t)$. (We will be using standard concepts such as random variables, density functions, independence and so on from the theory of probability and random variables [14, 13, 4].) The concept of time-to-compromise is based on the premise that any node is ultimately compromisable and the time when an attacker achieves the compromise is a random variable (which can include the attacker's skill level, choice of attack strategies and so on).

For example, the time to achieve success in a brute force attack on a key would be distributed according to a uniform density between time 0 (when the attack starts) and time N/M where there are N possible passwords and M random passwords tried per time unit. Techniques for estimating f_i and t_i for more complex computing systems have been developed and evaluated by the authors [2]. Moreover, estimates of the time-to-compromise density, $f_i(t)$, allows one to estimate the cost to compromise of the ith component as well as the overall system or mission [2]. Figure 1 has an example of such a time-to-compromise density.

The notion of time-to-compromise is directly analogous with the concept of time-to-failure in reliability theory [5]. The key difference is that reliability theory models component failures primarily as natural events whereas cyber security models attacks as deliberate adversarial activities undertaken by skilled human agents. A simple consequence of this is that two identical components will fail at independently distributed times whereas two identical cyber components will be compromised at highly correlated times typically. This key difference is the basis for much of what follows.

It is important to note that the time-to-failure of a component from a reliability point of view provides upper bounds on the time to achieve availability attacks. An intelligent adversary can only reduce the time to failure. There are examples in which a natural component failure, such as of a phyics based random number generator, could impact integrity and confidentiality as well but we do not pursue that in this paper.

2.3 Diversity

A variety of cyber security philosophies advocate deliberately engineering diversity into computer, network and information systems [7, 12, 3, 20]. Generally speaking, the goal is to address the *Monoculture Problem* which posits that implementations of complex cyber systems involving only single component types will allow an attacker to compromise all components once a technique is found to compromise any one of them. Diversity of component types suggests that compromising one does not allow the attacker to immediately compromise the others - additional, independent effort is required for each component.

It has been observed that there are different types of diversity and those different types may be appropriate for mitigating different classes of attacks [16]. Furthermore, the concept of cyber *moving targets* [7, 12] includes not only diversity but the ability of components and networks to change or morph over time so they do not present a stationary target to the attacker. Although we do not explicitly discuss this notion of diversity, we do believe that the techniques we develop are equally applicable to that concept as well.

It has also been noted that diversity as a cyber security strategy can come at a cost [3]. Monocultures are easier and more efficient to maintain. They generally scale better and offer the potential for improved interoperability and productivity. Recent work (see for example [8, 16]) has argued however that monocultures offer decreased security in the context of sophisticated, well resourced and targeted attacks. That work, however, is largely narrative and not quantitative, shedding little if any light on just how to quantify and evaluate diversity when it is deployed.

We propose to quantify the concepts of "monoculture" and "diversity" in terms of the type of joint probability function

$$f_{1,2,\ldots,n}(t_1, t_2, ..., t_n)$$

describing the time-to-compromise random variables, t_i, of the ith node or component in the system. By compromise, we mean that an attacker achieves his goal of gaining appropriate access to and privileges on a node. The time-to-compromise of a node is a random variable whose probability density can be determined analytically (such as in the case of attacks against a cryptosystem in which brute force at-

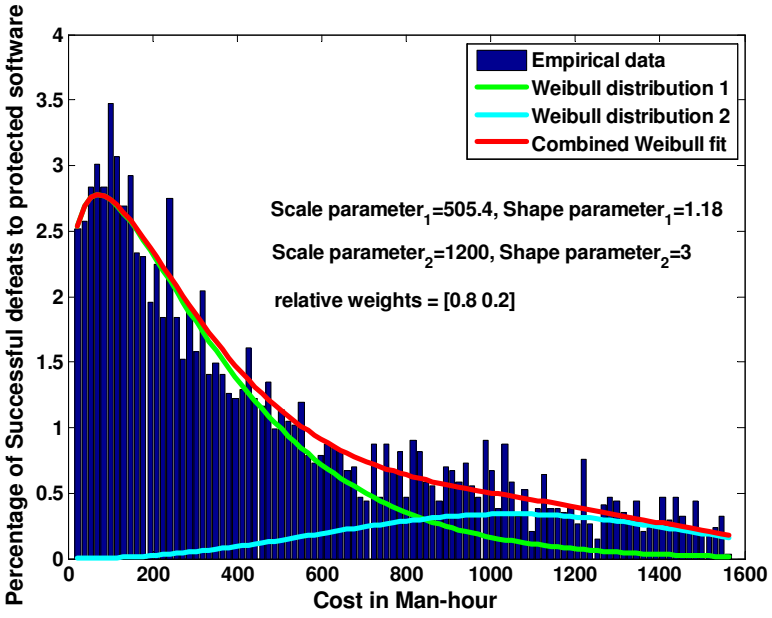

Figure 1: This figure depicts an example time-to-compromise density function developed by the authors in previous work [2]. The horizontal axis is time (equated to cost in man-hours here) while the vertical axis is the percentage of attempts requiring the corresponding time. The empirical probability density function was estimated using the QuERIES methodology [2] and is depicted by the blue bars. The red curve shows a Weibull mixture fit to the data with the mixture components shown in green and light blue. Weibull distributions are commonly used in reliability engineering to model component failures in non-adversarial environments [5]. The specific compromise that was modeled in this example was an attack against a protected software system by an adversary whose goal is to extract specific parameter values from the protected code.

tacks, are the only known option) or empirically) through red teams or information markets [2]) as discussed above.

Loosey speaking, $f_{1,2,\ldots,n}(t_1, t_2, ..., t_n)$ describes the probability distribution for when the various components of the system are compromised successfully. Readers unfamiliar with this concept are encouraged to review standard probability texts [14, 13, 4].

A monoculture has a joint time-to-compromise probability density function, $f_{1\ldots n}(t)$, that is not factorable into the marginal density functions. This is developed and explained further below but at this point we note that the factorizability of the joint density function is precisely the definition of "independence" in probability theory.

In other words, each node's time-to-compromise is not distributed independently of the other nodes' time-to-compromise. Typically, a monoculture is viewed as having the property that the attacker learns with the first compromise resulting in a reduction in the subsequent time needed to compromise other nodes. However, as we illustrate below, other systems with dependent, identically distributed times-to-compromise can result in the opposite situation. Specifically, if the system has very strong monitoring capabilities that can detect when one component has been compromised, the other components can respond with a higher security profile (ports and services shutdown for example) so that further compromises take much longer.

By contrast, diversity strategies aim to create independently or non-identically distributed times-to-compromise, or both. Independence means that an attacker gains little or no advantage from one successful attack to the next. A system having non-identical distributions means that each node has a different distribution of time-to-compromise. In particular, we call *natural* diversity the case in which all nodes have independent and non-identical distributed time-to-compromise probability density functions.

There are two distinct dimensions to diversity. The first is the dependence, in a probabilistic sense, of the time-to-compromise variables on each other. If they are independent random variables, we call the systems independent. If the compromise of one node affects the time-to-compromise of other nodes, we call the nodes dependent.

The second dimension is whether the nodes are homogeneous (operationally the same) or heterogeneous (operationally different). Mathematically, this is an assertion of whether the marginal times-to-compromise are identical or not as explained further below.

	Dependent	Independent
Homogeneous (Identical)	Monoculture (No Diversity)	Artificial Diversity
Heterogeneous (Non-identical)	Pseudo Diversity	Natural (True) Diversity

Figure 2: Diversity, or the lack thereof, can be partitioned into four quadrants according to whether the components are the same (Homogeneous), different (Heterogeneous), have time-to-compromise probabilities that are dependent or independent. Systems comprised of dependent and homogeneous nodes are monocultures while systems comprised of heterogeneous and independent nodes are called *natural* as in "natural" biological systems.

The marginal density for time-to-compromise of the ith node is

$$f_i(t_i) = \int_0^\infty ... \int_0^\infty f_{1,2,...,n}(t_1, t_2, ..., t_n) dt_1 ... dt_{i-1} dt_{i+1} ... dt_n$$

and can be interpreted as the probability distribution of time-to-compromise of the ith node irrespective of when other nodes are compromised. Whether $f_i(t) = f(t)$ for all i or $f_i(t) \neq f_j(t)$ for $i \neq j$ is the distinction between the homogeneous and heterogeneous cases respectively.

In terms of the joint density, we can therefore define the various possibilities in Figure 2 as follows:

Monoculture

$$f_i(t) = f(t) \text{ for all } i \text{ and } f_{1,2,...,n}(t_1, t_2, ..., t_n) \neq \prod_{i=1}^{n} f(t_i)$$

Artificial Diversity

$$f_i(t) = f(t) \text{ for all } i \text{ and } f_{1,2,...,n}(t_1, t_2, ..., t_n) = \prod_{i=1}^{n} f(t_i)$$

Pseudo Diversity

$$f_i(t) \neq f_j(t) \text{ for all } i \neq j \text{ and } f_{1,2,...,n}(t_1, t_2, ..., t_n) \neq \prod_{i=1}^{n} f_i(t_i)$$

Natural Diversity

$$f_i(t) \neq f_j(t) \text{ for all } i \neq j \text{ and } f_{1,2,...,n}(t_1, t_2, ..., t_n) = \prod_{i=1}^{n} f_i(t_i)$$

These concepts are relative to a specific attack and attacker type which will be made clearer in the following discussion with illustrative examples. The table in Figure 2 summarizes our taxonomy.

2.3.1 Monocultures

A *monoculture* system is comprised of nodes or components that each have the same time-to-compromise probability density function, namely $f_i(t) = f(t)$, and, most importantly, has the property that a successful compromise of any one node affects the subsequent time-to-compromise of other nodes in the system. In terms of the joint density function describing the time-to-compromise random variables for all n nodes,

$$f_{1,2,...,n}(t_1, t_2, ..., t_n) \neq \prod_{i=1}^{n} f(t_i)$$

which is precisely the probabilistic definition of dependence as applied to times-to-compromise.

Examples of such monocultures are computers sharing the same administrator password so that compromising the first machine in a brute force password attack takes some effort, subsequent compromises are essentially immediate. Similarly, a network consisting of nodes with identical operating systems and configurations will be a monoculture with respect to technical attacks against the configuration or operating system [16].

One manifestation of the dependency between the time-to-compromise variables in a monoculture is that they are clustered closely. The typical probability density function for time-to-compromise for such a monoculture has high probability concentrated around the line $t_1 = t_2 = t_n$. This situation is depicted in Figure 3.

Another manifestation of a possible dependency is that it takes much longer to compromise the second and subsequent components after the first is compromised, such as in the case of highly monitored, reactive systems. In that case, there is little probability anywhere around the diagonal (see Figure 4 for example).

2.3.2 Natural Diversity

A system with *natural diversity* is comprised of nodes or components that each have different time-to-compromise densities and additionally has the property that successfully compromising any number of nodes does not allow the attacker to more easily compromise any other nodes in the system. Attacking each node is a novel activity and the time for an attack to succeed is a random variable governed solely by the node's specific time-to-compromise density. An example of a system with natural (true) diversity is a system in which each node is running a different operating system with different implementations of services and interfaces and the attack is *not* against a common protocol vulnerability. This notion of "true" diversity, in the context of a specific attack, is consistent with previous definitions [16].

2.3.3 Pseudo Diversity

A system with *pseudo diversity* is comprised of nodes or components that each have different time-to-compromise densities and successfully compromising a nodes does change the time-to-compromise for other remaining nodes in the system. Attacking each node is a different activity but the time for an attack to succeed against another node is a random variable that does depend on previous sucessful attacks.

An example of a system with pseudo diversity is for example the banking system in which each node (bank) uses some proprietary systems and configurations leading to different implementations of services and interfaces. Attacks against specific banks have different time-to-compromise densities but because the underlying business domain, workflows and

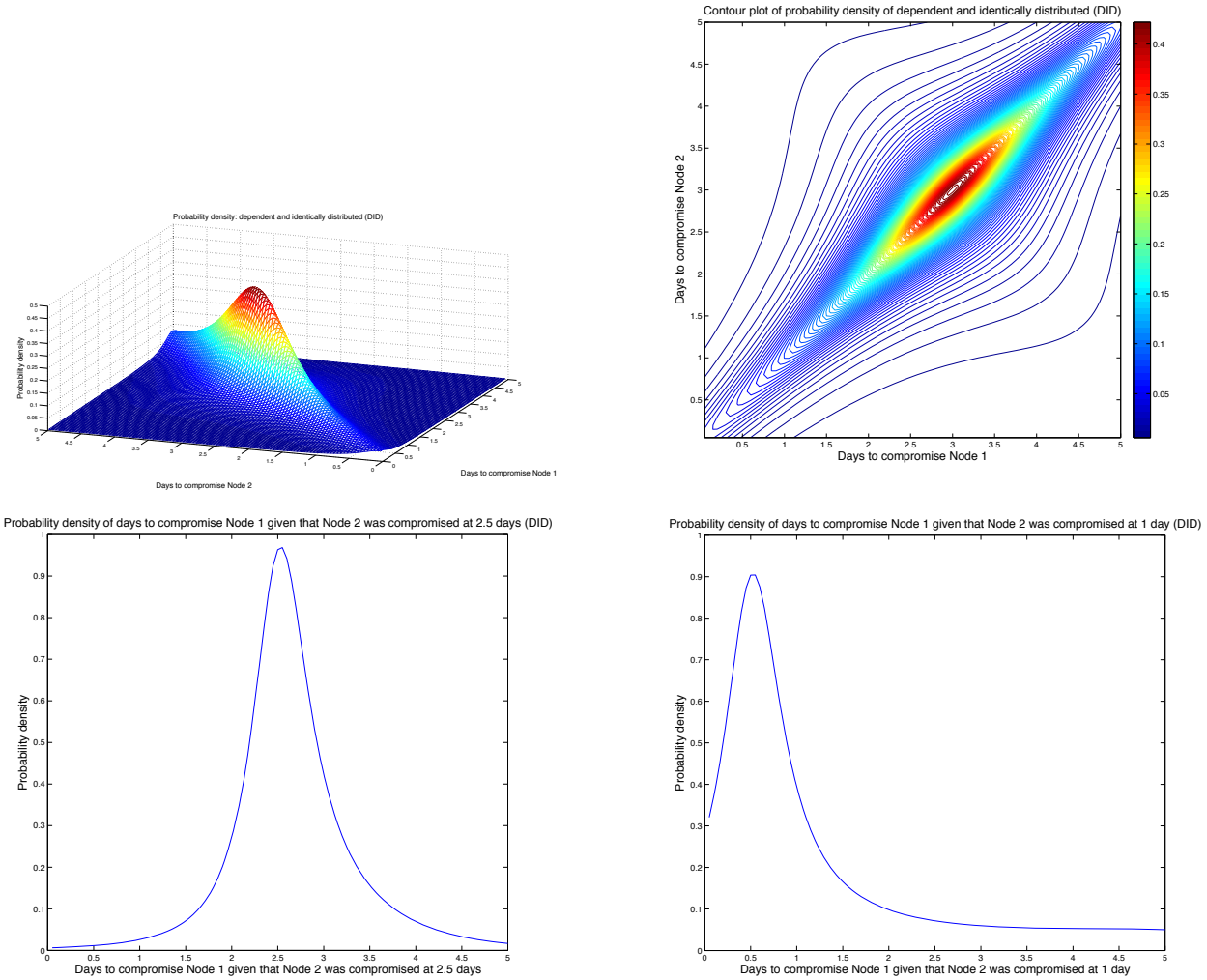

Figure 3: These figures depict a homogeneous and dependent time-to-compromise (Monoculture) probability density function for two nodes. The top left is a plot of the density. The top right is a contour map. The bottom left is a plot of the conditional probability $f_1(t|t_2 = 2.5)$ while the bottom right is a plot of $f_1(t|t_2 = 1)$. Because this example has dependent but homogeneous components, the two conditional time-to-compromise functions are not identical. That is, the time-to-compromise of one component does depend on when the other component was compromised and the compromise times are expected to be very close to each other. We will refer to this as a *classical* monoculture.

services that different banks employ are similar, an attacker will learn from one attack and be able to parley that into higher efficiency in the next bank they target. There is anecdotal evidence of this sort of pseudo diversity precisely in what have been called "beta attacks" .[1]

2.3.4 *Artificial Diversity*

Finally, a system with *artificial diversity* is comprised of nodes or components that each have the same time-to-compromise densities and additionally has the property that each attack's success time is independent of the others. Attacking each node is a similar activity and the time for an attack to succeed is a random variable governed by a common time-to-compromise density.

An example of a system with artificial diversity is a system in which nodes have implemented *address space layout randomization* (ASLR) [17], for example. An example of such a density is depicted in various ways in Figure 5.

2.3.5 *Limits to Diversity*

There are interesting and nontrivial results about the limits of diversity that can arise in natural populations [11, 10, 1]. Intuitively, consider an environment consisting of s possible species, constrained by or competing for c resources (for example, space requirements, cost of maintaining the species, total power consumption, administrative expertise

[1] 'Telltale signs of APTs can be identified through attacks on others: attendees observed a rise in "beta attacks" – adversaries attacking third parties simply to beta test techniques to be used on actual targets.' [15]

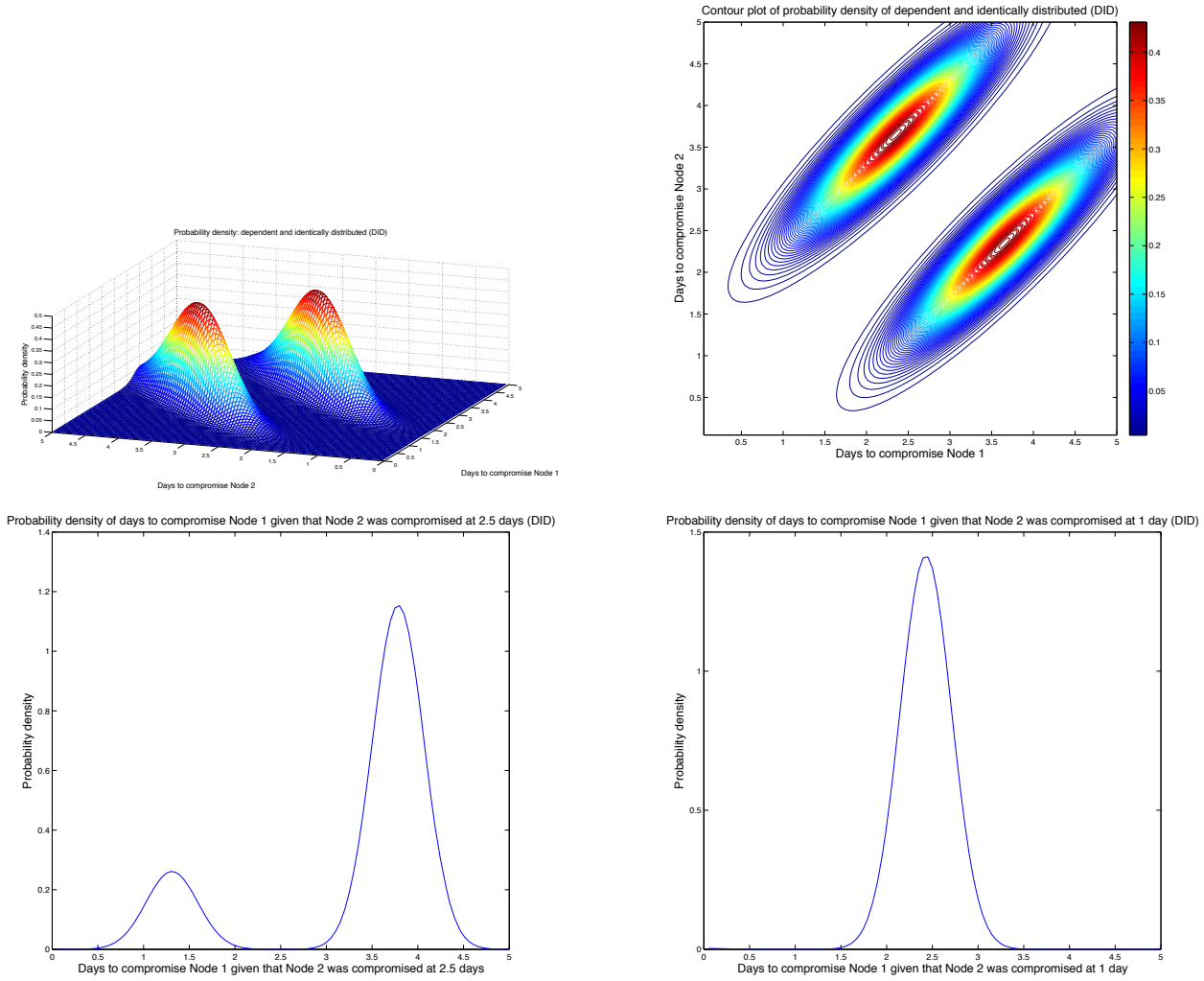

Figure 4: These figures depict another homogeneous and dependent (Monoculture) time-to-compromise probability density function for two nodes. The top left is a plot of the density. The top right is a contour map. The bottom left is a plot of the conditional probability $f_1(t|t_2 = 2.5)$ while the bottom right is a plot of $f_1(t|t_2 = 1)$. Because this example has dependent but homogeneous components, the two conditional time-to-compromise functions are not identical. That is, the time-to-compromise of one component does depend on when the other component was compromised and the compromise times are highly separated because of defensive measures introduced after the first compromise. We will refer to this as a *coordinated* monoculture.

and so on). Under many conditions, it must be that $s \leq c$ in the limit, meaning that unbounded diversity cannot exist naturally in competitive markets or economic environments. We are not aware of any empirical or theoretical evaluations of this property in computational systems involving diversity or moving targets but it would appear to be an interesting area to investigate in the future. Specifically, why are there only a handful of viable operating systems at any given time?

3. MAIN RESULTS

Our main results concern how long it takes a single or multiple attackers to achieve different goals, including compromising the classical CIA properties, against monocultures as well as systems with different types of diversity as described above.

We now develop consequences of these different types of system implementations with respect to a single attacker or multiple attackers seeking to achieve one of the CIA properties as special cases.

The key difference between a single, sequential attacker and multiple, parallel attackers has to do with the manner in which the various CIA goals are achieved as a function of the times-to-compromise of individual nodes or components.

In particular, a single, serial attacker adds the appropriate times so that the time to defeat node i first followed by node j is

$$t_i + t_{j:t_i}$$

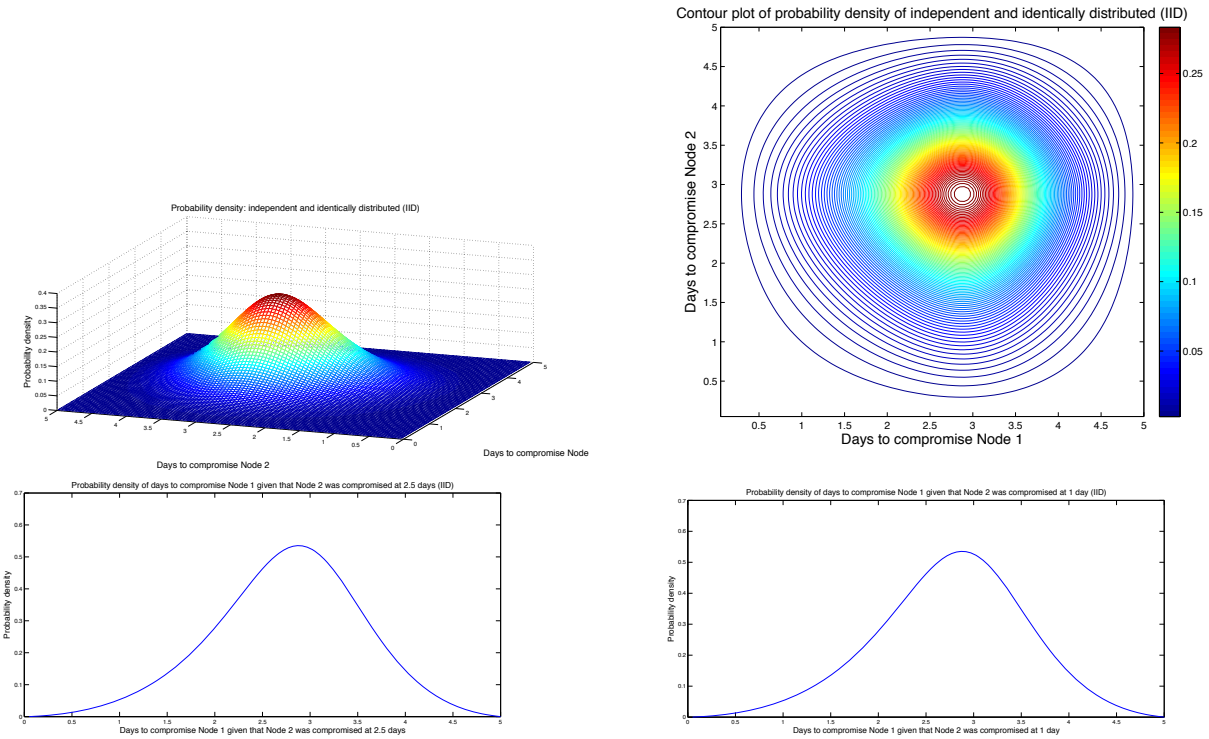

Figure 5: These figures depict a homogeneous and independent (Artificial Diversity) time-to-compromise probability density function for two nodes. The top left is a plot of the density. The top right is a contour map. The bottom left is a plot of the conditional probability $f_1(t|t_2 = 2.5)$ while the bottom right is a plot of $f_1(t|t_2 = 1)$. Because this example has independent but homogeneous components, the two conditional time-to-compromise functions are identical. That is, the time-to-compromise of one component does not depend on when the other component was compromised.

where $t_{j:t_i}$ is the random variable with probability density function

$$f_{j:i}(t_j) = f(t_j|t_i) = f_{i,j}(t_I, t_J)/f_i(t_i)$$

with the standard marginal distributions on the right hand side of the equation. Similarly, we define the times to defeat the first k nodes by a single, serial attacker as

$$t_1 + t_{2:t_1} + t_{3:t_1,t_2} + ... + t_{k:t_1,t_2,...t_{k-1}}.$$

The conditional distributions depend on the type of dependencies of course.

Multiple, parallel attackers on the other hand attack nodes in parallel with success time $t_1, ..., t_n$ and they defeat confidentiality, integrity and availability at times $t_{(1)}$, $t_{(n/2)}$ and $t_{(n)}$ respectively where $t_{(i)}$ is the ith order statistic. In parallel attack, times are not additive. Moreover, we assume that the number of potential attackers is the same order of magnitude as the diversity in the system under study.

3.1 Single Attacker Scenarios

In the case of attacks against confidentiality, a single attacker selects a node or component, i, and generates a sample of t_i, the time-to-compromise node i.

In the case of attacks against integrity, a single attacker selects $n/2$ nodes, $i_1, i_2, ..., i_{n/2}$, and generates the samples $t_{i_1}, ..., t_{i_{n/2}}$, of the times-to-compromise whose distribution is described by $f_{1,2,...,n}$.

In the case of attacks against availability, a single attacker must sample all n nodes and in doing so generates the samples $t_1, ..., t_n$, of the times-to-compromise whose distribution is described by $f_{1,2,...,n}$.

3.2 A Single, Sequential Attacker against a Classical Monoculture

These results assume that attacks are serial in that one component is attacked at a time. However, because of the classical monoculture assumption, a successful attack against one node can immediately be used against other nodes in the monoculture with minimal effort, for example in an automated and distributed attack.

We use

$$\mu_i = \int_0^\infty t f_i(t)dt = \int_0^\infty t f(t)dt = \mu$$

to denote the expected value of the time-to-compromise the ith node. In a classical homogeneous system such as are considering here, $\mu_i = \mu$, by definition.

Recall that a classical monoculture involves dependent, identically distributed times-to-compromise with the property that the dependency makes all nodes compromised shortly after the first.

3.2.1 Confidentiality

The time-to-compromise any one of the components by a single attacker is a single sample of the random variable distributed according to $f(t)$. It has expected value or mean μ which, according to our assumptions, is the time for compromising only one node, namely μ.

3.2.2 Integrity

The time to compromise the integrity of $n/2$ components by a single attacker in a classical monoculture is the time it takes to compromise one node and automate the attack against the other nodes. For simplicty, we assume that the time to compromise the other nodes in significantly smaller than the time to compromise the first node so 2 nodes would require an expected time of μ as well and so on. In particular, for $n/2$ nodes this is μ, the distribution's mean as above. The argument is made more formally in the Appendix.

3.2.3 Availability

The time to compromise availability of all n components by a single attacker in a monoculture is the time it takes to compromise one node and automate the attack against the other nodes, as above. As above, this is approximated by μ also. The argument is made more formal in the Appendix.

3.3 A Single, Sequential Attacker against Artificial Diversity

These results assume that attacks are serial in that one component is attacked at a time. This could be the result of resource limitations on the attacker side or an operational decision by the attacker to devote all resources to one node (component) at a time.

This is the best case scenario for the defender. Since a serialization of the attack results in a maximum expenditure of effort and hence maximum cost of the attack. The single, sequential attacker serves as an upper bound on the value of diversity as a stand alone security strategy. One wouldn't want to expend more on implementing diversity than this.

Recall that artificial diversity involves independent, identically distributed times-to-compromise.

3.3.1 Confidentiality

The time to compromise any component i by a single attacker is a single sample of the random variable distributed according to $f(t)$. It has mean μ so the expected time to defeat confidentiality is simply μ.

3.3.2 Integrity

The time to compromise $n/2$ components by a single attacker is the sum of $n/2$ samples of the independent random variables distributed according to $f(t)$. It has mean $n\mu/2$ so the expected time to defeat integrity is simply $n\mu/2$ for large n.

3.3.3 Availability

The time to compromise all n components by a single attacker is the sum of n samples of the independent random variables distributed according to $f(t)$. It has mean $n\mu$ so the expected time to defeat integrity is simply $n\mu$.

3.4 A Single, Sequential Attacker against Pseudo Diversity

These results assume that attacks are serial in that one component is attacked at a time. This could be the result of resource limitations on the attacker's side or an operational decision by the attacker to devote all resources to one node (component) at a time. As argued above, this is the best case scenario for the defender and an upper bound on the value of pseudo diversity.

Recall that pseudo diversity involves dependent, non-identically distributed times-to-compromise.

3.4.1 Confidentiality

The time to compromise any component i by a single attacker is a single sample of the random variable distributed according to the marginal density $f_i(t)$. It has mean μ_i so the expected time to defeat confidentiality by compromising the ith component is μ_i. Assuming the attacker selects one of the n nodes without a priori knowledge of which is which, the expected time to defeat confidentiality is

$$\frac{\sum_{i=1}^{n} \mu_i}{n}$$

which is the same as the natural diversity case.

3.4.2 Integrity

The expected time-to-compromise integrity for a single attacker on $n/2$ nodes in an n node system with pseudo diversity is the $n/2$ order statistic, $t_{(n/2)}$, of a sample $t_1, ..., t_n$ of the the dependent time-to-compromise random variables. The expected value of $t_{(n/2)}$ has an analytic express given by

$$E(t_{(n/2)}) = \int_0^\infty t f_{(n/2)}(t) dt$$

where

$$f_{(n/2)}(t) = \frac{d}{dt} \sum_{m=n/2}^{n} (-1)^{m-n/2} \begin{pmatrix} m-1 \\ n/2-1 \end{pmatrix} \cdot \sum_{1 \le i_1 < i_2 < ... < i_{n/2} \le n} F_{i_1, i_2, ..., i_m}(t, t, ...t)$$

where $F_{i_1, i_2, ..., i_m}(t, t, ...t)$ is the joint cumulative distribution of $t_{i_1}, ..., t_{i_m}$ [6].

3.4.3 Availability

The expected time-to-compromise availability for a single attacker on n nodes in an n node system with pseudo diversity is the n order statistic, $t_{(n)}$, of a sample $t_1, ..., t_n$ of the the dependent time-to-compromise random variables. The expected value of $t_{(n)}$ has an analytic express given by

$$E(t_{(n)}) = \int_0^\infty t f_{(n)}(t) dt$$

where

$$f_{(n)}(t) = \frac{d}{dt} F_{1,2,...,n}(t, t, ...t)$$

where $F_{1,2,...,n}(t, t, ...t)$ is the joint cumulative distribution of $t_1, ..., t_n$ [6].

3.5 A Single, Sequential Attacker against Natural Diversity

These results assume that attacks are serial in that one component is attacked at a time. This could be the result of resource limitations on the attacker's side or an operational decision by the attacker to devote all resources to one node (component) at a time. As argued above, this is the best case scenario for the defender and an upper bound on the value of natural diversity.

Recall that natural diversity involves independent, non-identically distributed times-to-compromise.

3.5.1 Confidentiality

The time to compromise any component i by a single attacker is a single sample of the random variable distributed according to $f_i(t)$. It has mean μ_i so the expected time to defeat confidentiality by compromising the ith component is μ_i. Assuming the attacker selects one of the n nodes without a priori knowledge of which is which, the expected time to defeat confidentiality is

$$\frac{\sum_{i=1}^{n} \mu_i}{n}.$$

3.5.2 Integrity

The expected time-to-compromise for a single attacker on $n/2$ components in an n node system with natural diversity is the sum of $n/2$ samples of the independent random variables distributed as in the confidentiality case. The expected value is

$$\frac{n}{2}\frac{\sum_{i=1}^{n} \mu_i}{n} = \frac{\sum_{i=1}^{n} \mu_i}{2}.$$

3.5.3 Availability

The time-to-compromise all n components by a single attacker is the sum of all n samples of the independent random variables distributed according to $f_i(t)$. It has mean

$$\sum_{i=1}^{n} \mu_i.$$

3.6 Multiple, Parallel Attacker Scenarios

In the case of attacks against confidentiality, n attackers select n different nodes or components and generate samples of t_i, the time-to-compromise node i. The time to defeat confidentiality is the first order statistic:

$$t_{(1)} = \min_i t_i.$$

In the case of parallel attacks against integrity, the attackers select all n nodes again and generate samples t_i, of the times-to-compromise whose distribution is described by $f_{1,2,\ldots,n}$ as above. The time-to-compromise integrity is the $n/2$ order statistic:

$$t_{(n/2)} = t_j$$

where $n/2$ values of t_i are less than or equal to t_j and $n/2-1$ values of t_i are greater than t_j.

In the case of parallel attacks against availability, n attackers attack in parallel all n nodes and in doing so generates samples $t_1, ..., t_{i_n}$, of the times-to-compromise whose distribution is described by $f_{1,2,\ldots,n}$. The time-to-compromise availability is the n order statistic:

$$t_{(n)} = \max_i t_i.$$

3.7 Multiple, Parallel Attackers against a Classical Monoculture

With parallel attackers against a classical monoculture, the time to defeat one of the CIA security goals depends on when the first, half, and last of the attacks are successful. The multiple parallel attacker scenario is most representative of a sophisticated nation-state actor with significant resources. In fact, this is probably the typical scenario at present given the implementation of current infrastructures.

3.7.1 Confidentiality

The time-to-compromise any component i in a classical monoculture by multiple, parallel attackers is the smallest of n samples of a random variable distributed according to $f(t)$. This is the 1st order statistic, $t_{(1)}$, and, as is shown in the Appendix,

$$E(T_{(1)}) \to \alpha \text{ as } n \to \infty$$

where α is the leftmost value in the support of f. That is, α is the largest value (supremum) for which $f(t) = 0$ for all $t < \alpha$. We include the possibility that $\alpha = 0$.

3.7.2 Integrity

The first time at which $n/2$ monoculture components can be compromised by multiple, parallel attackers is also the 1st order statistic of n independent samples of a random variable distributed according to $f(t)$ because, as before, once one node is compromised, $n/2$ can be quickly compromised as well. Therefore, the expected time to defeat integrity by a parallel attack is also α for large a large number of attackers n.

3.7.3 Availability

As above, the first time at which n monoculture components can be compromised by multiple, parallel attackers is also the 1st order statistic of n independent samples of a random variable distributed according to $f(t)$ because, as above, once one node is compromised, n can be quickly compromised as well. Therefore, the expected time to defeat availability in a monoculture by a parallel attack is also α for large a large number of attackers and nodes, n.

3.8 Multiple, Parallel Attackers against Natural Diversity

The analysis gets interesting because with parallel attackers, the time to defeat one of the CIA security goals depends on when the first, half, and last of the attacks are successful. The multiple parallel attacker scenario is probably representative of a sophisticated nation-state actor with significant resources. In fact, this is the more likely scenario and places a more reasonable bound on the value of diversity as a security strategy. One could argue that the time to compromise (and hence the cost to compromise) a system for the following security goals is an upper bound on the value of implementing *artificial* diversity in a monoculture.

We assume there are n diverse nodes and at least n attackers although they can only attack n nodes in parallel. Our results are relevant for large n since they involve limiting distributions.

3.8.1 Confidentiality

The time-to-compromise a component i by multiple, parallel attackers is the smallest of n time-to-compromise sam-

ples t_i distributed according to $f_i(t)$. That is, the time-to-compromise confidentiality is $t_{(1)} = \min_i t_i$.

The expected value of $t_{(1)}$ has an analytic express given by

$$E(t_{(1)}) = \int_0^\infty t f_{(1)}(t) dt$$

where

$$f_{(1)}(t) = \frac{d}{dt} \sum_{m=1}^{n} (-1)^{m-1} \sum_{i=1}^{n} F_i(t)$$

where $F_i(t)$ is the cumulative distribution of t_i [6].

3.8.2 Integrity

The first time at which $n/2$ components are compromised by multiple, parallel attackers is the $n/2$ order statistic, $t_{(n/2)}$, of a sample $t_1, ..., t_n$ of the the dependent time-to-compromise random variables. The expected value of $t_{(n/2)}$ has an analytic express given by

$$E(t_{(n/2)}) = \int_0^\infty t f_{(n/2)}(t) dt$$

where

$$f_{(n/2)}(t) = \frac{d}{dt} \sum_{m=n/2}^{n} (-1)^{m-n/2} \left(\begin{array}{c} m-1 \\ n/2-1 \end{array} \right) \cdot \sum_{1 \le i_1 < i_2 < ... < i_{n/2} \le n} \prod_{j=1}^{m} F_{i_j}(t)$$

where $F_i(t)$ is the cumulative distribution of t_i [6].

3.8.3 Availability

The time to compromise all n components by multiple attackers is the largest of n samples of the independent random variables distributed according to $f(t)$.

This is the n order statistic, $t_{(n)}$, of a sample $t_1, ..., t_n$ of the the dependent time-to-compromise random variables. The expected value of $t_{(n)}$ has an analytic express given by

$$E(t_{(n)}) = \int_0^\infty t f_{(n)}(t) dt$$

where

$$f_{(n)}(t) = \frac{d}{dt} \prod_{i=1}^{n} F_i(t)$$

where $F_i(t)$ is the cumulative distribution of t_i [6].

3.9 Multiple, Parallel Attackers against Artificial Diversity

Now the analysis gets interesting because with parallel attackers, the time to defeat one of the CIA security goals depends on when the first, half, and last of the attacks are successful. The multiple parallel attacker scenario is probably representative of a sophisticated nation-state actor with significant resources. In fact, this is the more likely scenario and places a more reasonable bound on the value of diversity as a security strategy. One could argue that the time to compromise (and hence the cost to compromise) a system for the following security goals is an upper bound on the value of implementing *artificial* diversity in a monoculture.

We assume there are n moving target, diverse, nodes and at least n attackers although they can only attack n nodes in parallel. Our results are relevant for large n since they involve limiting distributions.

3.9.1 Confidentiality

The time to compromise any component i by multiple, parallel attackers is the smallest of n samples of a random variable distributed according to $f(t)$. This is the 1st order statistic, $t_{(1)}$, and, as is shown in the technical section of this paper,

$$E(T_{(1)}) \to \alpha \text{ as } n \to \infty$$

where α is the leftmost value in the support of f. That is, α is the largest value (supremum) for which $f(t) = 0$ for all $t < \alpha$. We include the possibility that $\alpha = 0$.

3.9.2 Integrity

The first time at which $n/2$ components are compromised by multiple, parallel attackers is the $n/2$ order statistic of n independent samples of a random variable distributed according to $f(t)$. It has mean m which is the median of f (so $\int_0^m f(t)\ dt = \int_m^\infty f(t) dt = 0.5$. The expected time to defeat integrity by a parallel attack is simply m.

3.9.3 Availability

The time to compromise all n components by multiple attackers is the largest of n samples of the independent random variables distributed according to $f(t)$. This is the nth order statistic, $t_{(n)}$, and, as is shown in the technical section of this paper,

$$E(T_{(n)}) \to \beta \text{ as } n \to \infty$$

where β is the rightmost value in the support of f. That is, β is the smallest value (infimum) for which $f(t) = 0$ for all $t > \beta$. We include the possibility that $\beta = \infty$.

4. SUMMARY AND CONCLUSIONS

We summarize the above findings in a table which allows for easy comparison. C, I and A stand for confidentiality, integrity and availability respectively.

Attackers	**Artificial Diversity**	C	I	A
1	1	μ	μ	μ
1	n	μ	$n\mu/2$	$n\mu$
n	1	α	α	α
n	n	α	m	β

The results in the table are for Articifical Diversity only because the pseudo and natural diversity situations are more complex to present simply although they have been discussed above.

Note that as we increase the number of attackers, n, the expected time to defeat confidentiality approaches the minimal possible time in the case of both a monoculture and artificial diversity. This situation is depicted in Figure 6.

We have presented an initial but realistic model of how diversity as introduced by various mechanisms, including moving target defenses, changes the expected time-to-success of an attack against a system of computers. The attacks can be against confidentiality, integrity or availability.

Acknowledgement: Support for this research was partially provided by Army Research Office award W911NF-13-1-0421.

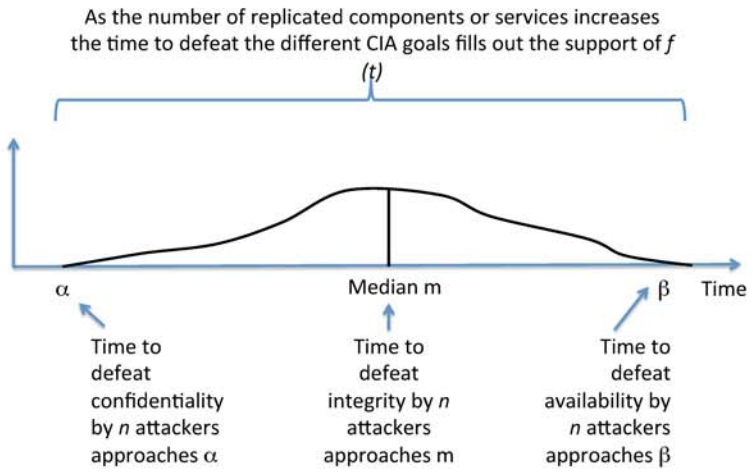

Figure 6: A system comprised of different components or devices, with similar "time to compromise" probability distributions, being attacked by n attackers will have different expected times to achieve different goals (Confidentiality, Integrity, Availability).

5. APPENDIX OF TECHNICAL DERIVATIONS

In this appendix, we present technical details about two of the four cases discussed above. The remaining two cases can be derived from these two examples using similar approaches.

A Single, Sequential Attacker against a Classical Monoculture

The intuitive notion of a classical monoculture is that once one node is compromised, other similar nodes in the system are compromised within a short period of time as well. This can be quantified by assuming that the joint density $f_{1,...,n}(t_1, ..., t_n)$ has the property that

$$f_{1,...,n}(t_1, ..., t_n) \neq 0 \text{ only if } |t_i - t_j| \leq \epsilon \text{ for all } 1 \leq i,\ j \leq n.$$

That is, all the probability is concentrated around the diagonal, $t_i = t_j$.

Under this model, a single attacker will succeed in attacking node i at time t_i where $|t_i - t_j| \leq \epsilon$ for all i and j. Therefore the $n/2$-th largest of the t_i, $t_{(n/2)}$, determines when the attack against integrity is completed and the largest, $t_{(n)}$, determines the time when the attack against availability is complete. Then

$$\begin{aligned}
\mu &= \int_0^\infty ... \int_0^\infty t_i f_{1,...,n}(t_1, ..., t_n) dt_1 ... dt_n \\
&\leq \int_0^\infty ... \int_0^\infty t_{(n/2)} f_{1,...,n}(t_1, ..., t_n) dt_1 ... dt_n = \mu_{(n/2)} \\
&\leq \int_0^\infty ... \int_0^\infty t_{(n/2)} f_{1,...,n}(t_1, ..., t_n) dt_1 ... dt_n = \mu_{(n)} \\
&\leq \int_0^\infty ... \int_0^\infty (t_i + \epsilon) f_{1,...,n}(t_1, ..., t_n) dt_1 ... dt_n = \mu + \epsilon
\end{aligned}$$

so if ϵ is small relative to μ, we note that $\mu + \epsilon \approx \mu$ which is the basis for the claims.

Multiple, Parallel Attackers against Artificial Diversity

Recall that artificial diversity is defined by

$$f_i(t) = f(t) \text{ for all } i \text{ and } f_{1,2,...,n}(t_1, t_2, ..., t_n) = \prod_{i=1}^{n} f(t_i)$$

so that times-to-compromise are independent and identically distributed.

Let $f_i(t)$ be the probability density function for the time to compromise the ith node of a system, t_i. The time for n attackers to defeat confidentiality is a random variable t_c that has cumulative probability distribution $F_c(t)$. By definition, t_c is the first "order statistic" [19] and $F_c(t)$ satisfies

$$1 - F_c(t) = Prob\{\text{all } t_i > t\} = \prod_i \int_t^\infty f_i(s) ds.$$

If all f_i are the same, so $f_i = f$, then

$$\begin{aligned}
f_c(t) &= dF_c(t)/dt \\
&= -\frac{d}{dt}(\int_t^\infty f(s) ds)^n \\
&= nf(t)(\int_t^\infty f(s) ds)^{n-1} = nf(t)(1 - F(t))^{n-1}.
\end{aligned}$$

Make the assumptions that $F(t)$ is continuous and that

$$\lim_{t \to \infty} t(1 - F(t)) = 0 \tag{1}$$

which holds for densities, $f(t)$, that have finite support or exponentially decreasing tails. The expected value of t_c dis-

tributed according to $f_c(t)$ is

$$\mu_c = E_c(t) = \int_0^\infty t f_c(t) dt \quad (2)$$

$$= n \int_0^\infty t f(t)(1 - F(t))^{n-1} dt \quad (3)$$

$$= -(t(1 - F(t))^n)|_{t=0}^\infty + \int_0^\infty (1 - F(t))^n dt \quad (4)$$

$$= \int_0^\infty (1 - F(t))^n dt \quad (5)$$

where we have used integration by parts to go from (3) to (4) and used (1) to obtain that the first term in (4) is 0.

Define α by $F(t) = 0$ for $0 \leq t \leq \alpha$, and $F(t) > 0$ for $t > \alpha$ which is well defined because F is continuous. In other words, the probability of compromise is nonzero only for times larger than α and can include the case $\alpha = 0$. Then $-(t(1 - F(t))^n)|_{t=0}^\infty = 0$ and

$$\int_0^\infty (1 - F(t))^n dt = \int_0^\alpha (1 - F(t))^n dt + \int_\alpha^\infty (1 - F(t))^n dt \to \alpha \text{ as } n \to \infty$$

because $1 - F(t) = 1$ for $t \leq \alpha$ and

$$\int_\alpha^\infty (1 - F(t))^n dt \to 0$$

as $n \to \infty$ by the Dominated Convergence Theorem. (Note that we have used

$$\int_\alpha^\infty 1 - F(t)\ dt \leq \int_0^\infty 1 - F(t)\ dt = t(1 - F(t))|_{t=0}^\infty + \int_0^\infty t f(t) dt = \mu < \infty,$$

$0 \leq 1 - F(t) \leq 1$ and $(1 - F(t))^n \to 0$ for $t > \alpha$ as $n \to \infty$.)

We can reduce the derivation of availability to confidentiality by noting that the time to defeat availability is the nth order statistic from n samples and applying the same mathematical derivation as above. Alternatively, by considering $s = 1/t$ as the random variable, we see that the expected time time to defeat availability is the smallest (first) order statistic of $1/t$ and so approaches β where $F(t) < 1$ for $t < \beta$ and $F(t) = 1$ for $t \geq \beta$ with the obvious interpretation when $\beta = \infty$.

The derivation for the time to defeat integrity can be reduced to a classical result by noting that in our model, half the nodes of the system must be compromised so that $t_i = t_{(n/2)}$ and $t_{(n/2)}$ is normally distributed with mean equal to the median, m, of f (that is, $F(m) = 0.5$) and variance equal to $\frac{1}{4nf(m)^2}$ [19].

6. REFERENCES

[1] R. Armstrong and R. McGehee. Competitive exclusion. *American Naturalist*, 115:151–170, Feb. 1980.

[2] L. Carin, G. Cybenko, and J. Hughes. Cybersecurity strategies: The queries methodology. *IEEE Computer*, pages 20–26, 2008.

[3] D. Evans, A. Nguyen-Tuong, and J. Knight. Effectiveness of moving target defenses. Chapter in Moving Target Defense: An Asymmetric Approach to Cyber Security edited by Sushil Jajodia, Planned for 2011.

[4] W. Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. Wiley, 3rd edition, 1968.

[5] I. Gertsbakh. *Statistical Reliability Theory*. Marcel Dekker, New York, 1989.

[6] M. Güngör, Y. Bulut, and S. Çalik. Distributions of order statistics. *Applied Mathematical Sciences*, 3:795–802, 2009.

[7] S. Jajodia, A. Ghosh, V. Swarup, C. Wang, and X. S. Wang. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer, New York, 2011.

[8] J. H. Lala and F. B. Schneider. IT monoculture security risks and defenses. *IEEE Security & Privacy*, 7(1):12 –13, Jan.-Feb. 2009.

[9] L. Lamport, R. Shostak, and M. L. Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4:382–401, July 1982.

[10] S. A. Levin. Community equilibria and stability, and an extension of the competitive exclusion principle. *American Naturalist*, 104:413–423, 1970.

[11] R. Macarthur and R. Levins. The limiting similarity, convergence, and divergence of coexisting species. *The American Naturalist*, 101(921):377–385, Sep.-Oct. 1967.

[12] NITRD. Moving targets. http://cybersecurity.nitrd.gov/page/moving-target, 2011.

[13] A. Papoulis. *Probability, Random Variables and Stochastic Processes*. McGraw-Hill, 2nd edition, 1984.

[14] S. M. Ross. *Probability Models, 9th Edition*. Academic Press, 2007.

[15] RSA. http://www.rsa.com/innovation/docs/APT_findings.pdf, 2011.

[16] F. B. Schneider and K. P. Birman. The monoculture risk put into context. *IEEE Security & Privacy*, 7(1), Jan.-Feb. 2009.

[17] H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pages 298–307, New York, NY, USA, 2004. ACM.

[18] S. Smith and J. Marchesini. *The Craft of System Security*. Addison Wesley, Upper Saddle River, NJ, 2008.

[19] S. S. Wilkes. Order statistics. *Bull. Amer. Math. Soc.*, 54:6–50, 1948.

[20] Williams et al. Security through diversity. *IEEE Security & Privacy*, 2009.