All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The DIE Model

I don't usually keep track of every new set of initials I see in cybersecurity because they are mostly about a breakthrough in marketing technology. But this one came up recently in a discussion forum I participate in sometimes, so I thought I would take a look at it.

Distributed, Immutable, Ephemeral

The first thing I notice about the DIE model is that it's intended to replace the CIA model (Confidentiality, Integrity, Availability) which already had a few problems including:

- These are objectives, which hardly constitutes a "model"
- CI and A are not enough, we currently use IACUTRS as protection objectives.[1]

Here's what the AI returned from my search:

- Distributed: Instead of a single, centralized target, systems are spread out. If one component is compromised, the entire system is not lost.
- Immutable: Assets cannot be modified after deployment. If a change is needed, a new, secure component is created instead of updating the old one, preventing tampering.
- Ephemeral: Components have a short lifespan. They exist only for as long as necessary, making it harder for attackers to maintain a persistent presence in the system

I don't necessarily think these are the right and proper definitions, not that there particularly are any, but I will go from here. According to another AI response:

> The DIE (Distributed, Immutable, Ephemeral) cybersecurity framework was authored by Sounil Yu and first appeared around 2020. … The concept was introduced by Yu in his 2020 presentation "Distributed Immutable Ephemeral – New Paradigms for the Next Era of Security" at the RSA Conference. … DIE focuses on increasing resilience by designing systems that are Distributed (no single point of failure), Immutable (cannot be changed), and Ephemeral (short-lived).

Good ideas, but...

These are interesting and often worthwhile objectives as properties of systems. But there are a few things I should point out:

- **Distributed** systems, while more resilient to many sorts of failures, are also potentially problematic for other sorts of failures. For example, if the content is distributed, that means either that you need access to multiple places to get the content you need or the content is replicated.
  - **If you need access to multiple places**, the system has more things that can go wrong rather than fewer (hopefully fault tolerant, but not fault intolerant).

1 https://all.net/Arch/index.html

  - **If the content is replicated** it means there are more places it can be leaked from (less assurance of confidentiality) and the cost of the replicas and keeping them consistent may be problematic.

- **Immutable** content or mechanisms are a great idea, especially for things like startup disks and hardware, but there are at least two problems; nothing is really immutable and for the most part we really don't want it to be, and this tends to mean that imperfections are not removable so they get exploited again and again.
  - Since **nothing is really immutable**, you have to be careful about using this as an assumption, and potentially replace it with the conditions under which it remains unchanged. I think we generally want some things to be immutable over some time frames and environmental conditions, and that this is a good idea.
  - **Imperfections never fixed** means that threat actors exploit the same things again and again. I am not a fan of making imperfect systems, but then I also don't know how to make anything perfect. But I do think we are too fast and loose with changes
- **Ephemeral** (short-lived) seems to me to be in opposition to immutable. Saying that we create things and then destroy them sounds to me like temporal microzones, which I am a fan of, wrote on their virtues[2], and included as a method (or set of methods) to be used in our standards of practice.[3] But having said that, there are situations when different components should or should not be ephemeral in nature, and they are complicated depending on consequence levels, risk aggregation issues, distribution properties, and so forth.
  - **Different things for different time periods**, which means "short" is a relative term, or in other words, horses for courses.
  - **Permanent presence spans component replacement**, especially in distributed attack methodologies. Computer viruses are one of the obvious examples of mechanisms that tend to survive the replacement of components since the new components are just new opportunities for infection.

Conclusions

I generally think that folks who jump on the DIE bandwagon are going to stay on that bandwagon for the rest of their time in the field, not because it's the best approach, but because it has 3 letters and is a nifty acronym. I like the underlying notions, agree with them as concepts that should be kept in mind, along with the hundreds of other things that should also be kept in mind.

But the problem with this approach is that people can really only remember 7+/-4 things in our chunked memories. And cybersecurity is more complicated than that.

DIE does not replace CIA, and in my view, neither of them should be used as a basis for decision-making without putting them in the larger context of the complex issues of real cybersecurity. But they do represent a breakthrough in marketing … something or another. I think it's good to look at things in different ways, and I hope DIE offers more light than heat.

2 https://all.net/Analyst/2015-03.pdf
3 https://all.net/SoP/SecDec/ZoneVirt.html

