All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The Design Basis Threat

This term of art poorly describes that there is a threat set identified as the basis for design. In other words, in order to defend, we must model what it is we are defending against. It may seem and be trivially obvious that designing against an unidentified and arbitrarily unknown threat makes design of effective protection infeasible, but this is an issue that is often and widely overlooked, leading to poorly specified and highly unbalanced defensive postures.

What is a threat set?

A threat is anything capable of acting against the desired operation of the system under study. Normally, we talk about humans (individuals and groups) and nature (other life forms and physical phenomena). When we discuss threats, it is fairly common to identify them in terms of capabilities and intents. Capabilities have to do with all of the things the threat brings with them to the table, while intent applies to human actors and some natural creatures. A tornado has “capabilities” in terms of the amount of wind and rain it can bring to bear and the sorts of things that the wind and water can do when interacting with other resources (e.g., tree branches and bird feathers may act like weapons at high velocity). But tornados don't have intent per se. Dogs, cats, and rats have intent, in that they can perform complex event sequences with goal-directed behaviors that may run counter to the desires of the defender, but in terms of design issues, their intent is typically not directly averse to human intents. Of course animals can be trained, and other mechanisms (e.g., robotics and programs) can be directed to act with the intent and coordination of the larger organizations they are part of.

A threat set is a set of representative threats intended to cover the space against which considerations are to be given. Typically, harsher threats cover all of the capabilities and intents of milder threats, so to the extent that more and more broadly capable and motivated applicable threats subsume lesser threats, we need only model the harsher threats in our analysis. There is also the issue of threat volumes and incident rates, which goes to the issue of resources and sequences, but we will not go further into this for now.

An example

An example of a design basis threat is given in the Nuclear Regulatory Commission's 10 CFR 73. Here is an extract regarding the consequence “(2) Theft or diversion of formula quantities of strategic special nuclear material.”

> “(i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes:
>
> > a single group attacking through one entry point,
> >
> > multiple groups attacking through one or more groups and one or individuals attacking through multiple entry points, (sic)
> >
> > or individuals attacking through separate entry points,

Copyright(c) Fred Cohen, 2012 - All Rights Reserved

with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including handheld automatic weapons, equipped with silencers and having effective long-range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safe-guards system;

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack."

In other words, at least one Navy SEAL teams with insider support and the full resources of a nation-state behind them, using the full spectrum of available tools and techniques. Of course your facility may not be this one, but you get the idea.

How do we develop a threat set?

One approach to developing a design basis threat associated with a set of consequences is to look at the history of threats from several angles. Typically, we look at common threats that are present for every similar situation (e.g., Internet connected systems are attacked by botnet herders), present within an industry or other vertical (e.g., innovative manufacturers are commonly attacked by competitors), specific company types (e.g., a company that makes fur coats will be targeted by animal rights activists), specific companies (e.g., disgruntled ex-employees and employees will attack companies undergoing substantial layoffs), and specific individuals (e.g., individuals may be targeted as a result of a legal action, recent death, etc.). All that apply are then characterized in terms of capabilities and intents, and greater threats that subsume the capabilities and intents of lesser threats are taken as representative, or a fused model is created. We commonly detail threats in terms of funding/attack, size, motives, skills, effort per attack, access, specific concerns, and history of incidents. We tend to associate motives from the set {Justice / Acceptance / Money / Malice / Insanity / Power / Patriotism / Revenge / Randomness / Exploration / Religion / Pride), access from the set {Insider/Partner/Industry/Internet}, and skill from {low, medium, high} in information protection threat identification efforts. Historical data is gathered as part of the effort of threat identification, and is part of diligence in identifying applicable threats.

Copyright(c) Fred Cohen, 2012 - All Rights Reserved

What do we do with a threat set once we have it?

Once we have a threat set, we may then associate them with consequences of import to the business, starting at the highest consequences and working our way down. If a threat set cannot produce a consequence based on its capabilities and intents, it is left out of that part of the analysis. But that's only the first step. For each considered consequence, we have to understand and analyze the threat set relative to defenses to determine what sets of defenses and residual risks are acceptable.

We typically use characteristic sets of attack mechanisms to detail what threats have the capacity to do, again, all based on best estimates of experts and their review of historical information and assessment of likely futures for the relevant time frames. We then produce a set of design basis threats, such as the one identified above, associated with different consequences of import. Of course we may only need one such threat if enough similar consequences arise with similar threats.

How do design basis threat and risk management inform each other?

In essence, risk management has to consider the tradeoff between things that the applicable threats may do and the costs of deterring, preventing, and detecting and responding, and find a set of protective measures and acceptable residual risks relative to those threats. Out of all of the potential protective schema, risk managers who are effective, typically find relatively inexpensive and effective protective schemes and determine reasonable places to accept risk. For example, a risk manager may look at the difficulty of preventing attack and decide that the design basis threat allows for the attack to succeed against one facility while preventing it against three redundant ones. If the redundant data center approach is more cost effective than the alternatives, or if data center redundancy is a part of the business plan regardless, they may identify this as an acceptable alternative to preventing the attack, and build the redundancy or merely accept the risk. Similarly, if the effect of outages over time are such that detection and response can mitigate in time to stop consequences in excess of risk acceptance thresholds, the risk manager may decide to put the money into capabilities to detect and respond, particularly as part of a larger detection and response program that already exists.

At a more strategic level, there are other factors that may come into play. For example, it may reasonably be determined by management that certain aspects of protection against certain threats are beyond the scope of their responsibility. It may be true that nuclear weapons will be able to destroy some set of facilities at some rate, but if you are a normal commercial enterprise, protection against nation states engaged in nuclear war is likely beyond the realm of things you should be protecting against. Rather, it is the role of government to provide for the common defense in this case. Of course if you are from government, you may indeed have the responsibility and may have to address that threat. Thus risk management should reasonably ignore some threats and embrace others. This is a matter of judgment.

Other threats may be less obvious. For example, if you manage risks for an element of critical infrastructure, there are almost certainly cases in which the same sorts of actors identified for nuclear facilities would be applicable against lower consequence facilities as part of a larger strategic attack plan. But any strategy other than an adequate response process involving government and private sector resources will produce far too high a cost against such a threat set in almost all cases. The design basis threat must be informed by these facts.

Copyright(c) Fred Cohen, 2012 - All Rights Reserved

The link between risk management, design basis threats, and protective schema

From a practical standpoint, no direct path exists today for turning a design basis threat into a protective scheme. Rather, the design basis threat is predominantly used today as part of a testing methodology for protective schema. A proposed scheme may be tested hypothetically or experimentally against the design basis threat to better understand the effectiveness of that protective scheme. In experimental tests, portions of the protective scheme, or the scheme as realized in a particular instance, are tested against actual or simulated threats. This tends to be expensive as the scale increases, and is thus done rarely and only in high consequence environments. In hypothetical cases, simulations or table-top exercises are typically used.

Of course real protective schemes are complicated and non-trivial to develop, and tests are expensive to perform, so risk managers usually have choices among a small number of alternatives. Again, as the value increases, the reasons for examining threats in more detail and the need to do so also increases. Management has a responsibility to understand these tradeoffs in regard to their own purview and make decisions about how far to go in their risk management program in terms of defining and analyzing protective schemes against design basis threats in the context of risk management. It is common practice to give only minimal attention to these threats and the examination of these issues, and this is often justified.

Summary

The notion of a design basis threat informs risk management. Without such a notion, a firm basis for decisions about protective schemes for high valued targets is hard to reasonably produce and justify. Lingering questions will remain of (1) whether we have protected against something that will almost certainly never happen and what price we have paid for that overprotection; and (2) whether we have provided adequate protection.

But there is a real cost to examining design basis threat in detail, and its use is not generally justified when consequences and threats are low. While this may seem circular, it is not. A nominal study of threats and consequences is commonly used as part of a protection posture assessment or similar process to gain perspective on the overall situation and identify cases in which higher quality threat assessment is required.

In architecting and designing protection for medium- to high-valued targets, the design basis threat is important to understand and consider, as it leads to limitations on available methods and forces minimum levels of consideration. Thus design basis threat sets a requirement that all viable alternatives must satisfy.

At the end of the day, risk managers choose between a fairly small number of alternatives. As a result, while design basis threat in medium or high risk situations is an important component of the analysis, it is only the differential between alternatives that ultimately leads to decisions.

Today, we have a term of art that is truly related to the art rather than science, produced by artisans, and usually without a testable methodology or widely accepted basis. But the fact that protection is an art should hardly be a surprise. The complexity and rapidly changing adversarial nature of the field seems to imply that competition will, for the foreseeable future, drive changing threats. And as the threats change, the need to better understand them and identify their capabilities and intents as part of the basis for design becomes increasingly apparent.

Copyright(c) Fred Cohen, 2012 - All Rights Reserved