Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Progress and evolution of critical infrastructure protection over the last 10 years?

Someone asked whether and to what extent critical infrastructure protection has improved in the last 10 years. It seems to me that while many changes can be readily identified, there is no basis today for determining whether or to what extent such changes have made protection more or less effective. The most fundamental change we need is to move toward a science of protection, and this has not been seriously undertaken, at least in the areas where I work. As a result of the lack of scientific study and a widely accepted scientific basis, I know of no way to make sensible measurements of protection quality as a whole, and improvement cannot be realistically assessed without such metrics. Some more detail might be in order.

What changes have been made

Many protection changes for critical infrastructures have been made in the last 15 years. Starting in the late 1990s when the President's Commission on Critical Infrastructure Protection (PCCIP) identified a national need to make protection changes, a vision of a future state was notionally present. But that vision was not then being realized at a rapid rate. Then the September 11, 2001 attacks on the US took place, leading ultimately to a dramatic change in the protection posture of the US and much of the rest of the World.

Unfortunately, to many knowledgeable and skeptical observers, many of these changes were of little technical value other than from a perception perspective. Things like increased levels of invasiveness and inconvenience in airport searches were not met by published or identified measurements of effectiveness. Testing showed repeatedly that the countermeasures could be readily bypassed, and a system of continuous “improvement” based on reducing the potential for the “last attack” were applied with little apparent effect other than to make travel less convenient, more costly, and more invasive to the traveling public, with perhaps a marginal but unmeasured (or unpublished) benefit in reducing copy-cat attacks. The feeling of safety (or lack thereof) and level of suspicion engendered by such measures has the – again unmeasured – likely effect of making individual and poorly trained threat actors more nervous and more likely to be detected and interdicted, while making the public at large feel safer (or more afraid), with benefits of these results quantitatively unknown and somewhat speculative.

Other less obvious changes were perhaps somewhat more technically effective, although again, measurement has not been widely published if it has been undertaken in a meaningful way at all. For example, water systems, pipelines, power systems, telecommunications, and other similar systems have been examined at some level of depth to better understand the potentials for harm and the limitations of existing protective mechanisms. While the increased scrutiny is, presumably, a benefit in terms of general and situational awareness, and the increased focus of attention and resources on these issues has the potential to increase the knowledge of the issues, evidence of the utility of these presumed benefits is lacking and no system of measurement has been widely identified and applied to provide meaningful metrics. Lacking a system of measurement and a standard against which to measure, it is doubtful that we can determine factually if protection is better or worse today than it was 10 years ago.

Some things we may be able to measure in some areas

By focussing on select areas of protection, additional insight may be gained. The particular areas of foci here are information protection for (1) general purpose computing at enterprises, by individuals, and in government, which is vital to several critical infrastructure sectors (e.g., finance, government, telecommunications, logistics), and (2) industrial control systems, which are vital to traditional critical infrastructure sectors (e.g., power, water, fuel, manufactured goods, transportation). Within these areas, some commonly considered issues are identified and discussed in terms of changes over the last 10 years. This represents only my qualitative assessment and is without adequate basis in measurement to be treated as definitive in any meaningful way. Measurement in these areas is currently problematic as discussed.

Risk issues:

- **Threats:** It appears that more and more skilled, organized, and resourced threat actors have been identified and are active in 2011 than in 2001. However, there is no systematic reporting of or method for identifying and characterizing such individuals and groups available in any public forum I am aware of. While there are groups that produce reports and provide databases on these issues, none of them appear to have base rates or methodologies to support sound conclusions about situation at any given time or as it changes with time.
- **Vulnerabilities:** It appears, based on publicly available databases like the OSVDB and CVE, that the rate of widely published vulnerabilities has increased, but this tends to ignore many of the widely known vulnerabilities that are not directly technical in nature, such as exploitations of people, systems, architectures, and similar issues. For example, malicious programs that are downloaded and run by users represent vulnerabilities that are ignored by most such collections and often dominate the events of interest. Interconnection and architectural vulnerabilities have increased for ICS systems so that it is clear that there are more paths to attack them. Many ICS systems don't have the same sorts of protection mechanisms feasible today as general purpose Internet connected computers, and this can reasonably be seen as an increase in vulnerability if measured in terms of the size and number of links from external sources to targets in the attack graph. But as a metric, it is unclear whether this is useful for understanding the overall situation. Similarly, things like the 'attack surface' metrics are poorly measured and have no real objective criteria or comprehensive application. Insiders remain responsible for much of the attributed damage, and thus external connectivity changes may be of relatively limited impact in terms of overall security.
- **Consequences:** The consequences of attacks are rarely available for review as they tend to be closely guarded secrets. While the widely publicized consequences are seemingly bigger and more frequent today than 10 years ago, as seen by the DataLoss.Org Web site and published reports, reporting requirements have increased as has publication of events. Reporting requirements today have limited metrics (i.e., number of people affected) and attend largely to only privacy and outages. When consequences are available, the lack of a common method of valuation for information-related losses or content leads to numbers that are often not comparable and thus fail to support any meaningful conclusions against a standard or over time.

- **Interdependencies and risk aggregation:** Analysis necessary to support definitive answers in this regard is again not available. But is seems almost certain that analysis would show that aggregation of risks and interdependencies have dramatically increased over the last 10 years. There is little available data to support substantial conclusions from losses in this regard, but the effects of risk aggregation and common mode failures have produced dramatic results like the nuclear reactor problems in Japan, the WikiLeaks incident, and many other large-scale events in the media. What is unclear is whether the situation is in fact getting worse. In addition to the lack of measurement, reports tend not to attend to risk aggregation or interdependency issues and those making such reports may be largely unaware of these issues. Even for reported cases, valuation methods are not available and quantification is not based on a standard. The rationale for asserting that the problem is worse is the increased complexity and integration of systems into larger and more complex mechanisms. For example, identity management has moved ahead substantially. Along with it, federation of identities and the use of centralized servers for control of these processes places increased risk on the small number of servers leveraged to larger effect and adds interdependencies that were not previously present. However, the economies of scale and quality of such systems may compensate for the aggregations by providing higher surety for more systems. Again, without a system of measurement, no basis for meaningful metrics can be supported.
- **Risk management approaches:** The four basic approaches, transfer, acceptance, avoidance, and mitigation, have not changed over the last 10 years, and this field appears to be relatively static. It may appear that the tolerance for risk has increased in the information arena, but this may be the result of a lack of understanding of the issues rather than a conscious or knowing decision by decision-makers.

Protection objectives:

- **Integrity** protection capabilities have improved to some extent in large numbers of computers as trusted computing group trusted platform module integrity mechanisms have been increasingly deployed over the last decade. But these mechanisms go largely unused for anything other than limited digital rights management. Meanwhile, systems like mobile devices, which are increasingly dominating the consumer market and pushing into enterprise markets, largely lack longstanding integrity mechanisms such as hardware process separation and file systems security. Again, we have no sound method for measuring any actual change in integrity protection.
- **Availability** of hardware has improved with technological advancements, and software checking has improved availability along with operating system improvements for widely deployed operating environments like Windows, but at the same time, server software has become more complex and interdependent, and no widely available measurements of availability have been identified that could address the overall question of availability. Furthermore, the movement to mobile devices has dramatically changed the nature of availability since access and utility has increased from a wide range of locations where access was previously very expensive and not widely available. Again, depending on what you choose to measure, different results will appear. It is, however, obvious to most observers that accessibility to services has

made a dramatic shift in the positive direction with the increased availability of WiFi and cellular services supporting smart-phones, pad computers, and netbook platforms.

- **Confidentiality** has been problematic in the rapid growth of Internet technologies and the push toward gaining efficiencies of scale. Many disclosures of high volume leaks have driven the perception of a worsening situation, but again, no comprehensive metrics are really available. Large-scale leakage of classified information to the media associated with the WikiLeaks case appears to be unprecedented, but it is unclear how this effects or relates to critical infrastructures or normal user situations.
- **Use control** is apparently being loosened as mobility increases and information work is increasingly outsourced and physically distributed. More and longer chains of interdependencies appear to be present today than 10 years ago, and this leads to use control problems that are increasingly seen in published attacks that gain access to user interfaces which are then exploited to attack systems the users have access to. But again, metrics in this area are lacking and the lack of detection does not translate into a lack of actual attack. More detections may mean fewer attacks persist.
- **Accountability** requirements are increasing in many systems and infrastructures as logging is being added and reporting mandates increase. Laws like Sarbanes-Oxley Act and the Gramm-Leech-Bliley Act are reflected globally, and the financial crisis has increased the recognition of the lack of accountability. But in truth, there was little accountability 10 years ago and little accountability today as exemplified by the inability to demonstrate or definitively determine ownership of millions of homes. The lowest level actors are punished for top-level acts of malice or incompetence, and the rich and powerful have gotten richer and more powerful over the last 10 years by avoiding accountability for a market collapse that was largely their fault and paid for by others.

Protective technologies and approaches:

Essentially no widespread new technologies for information protection were deployed in the last 10 years. Identity management has increased market penetration, data loss prevention methods similar to previous methods for intrusion detection have become more widespread, trusted platform modules are more widespread, but the overall effect of these changes is apparently negligible and no metrics accurately measure any such effects today. Technologies supporting ICS security are essentially unchanged over this period despite dramatic increases in connectivity and movement toward lower surety platforms. This does not bode well for protection of these elements of critical infrastructures. We see more spending on protection, but again, without metrics, ...

Conclusions:

The science and measurement associated with information protection has not yet reached the point where even the most basic questions about whether protection is better or worse can be meaningfully evaluated. Without developing a science and system of measurement, we won't be able to answer these sorts of questions 10 years from now either. The main area where we need to make progress in order to make progress in all other areas, is an area where we have made little or no progress. And time is not on our side.

