19-601, Spring 2002
Homework 4

Daniel M. Vogel

March 5, 2002

Abstract

We are a limited resources, physically distant entity with a strong personal animosity towards Bunkered. It is not defined as to the nature of this animosity, and yet to the offensive scenerio, this is critical. To demonstrate this, I propose three motivational scenerios with offensive and defensive countermeasures. Through incremented offensives spaced apart, the Evil attacker may exploit the core weaknesses inherent in any legitimate organization: human weaknesses, customer responsibility, public opinion, and trust. Some proposed policy and defensive measures, drawn from Underground practices, are suggested.

1 Strategy

I will present the strategic discussions in a classic format: with quotes from *The Art of War*[1] followed by applicable commentary. Blockquotes in san-serif indicate language from the scenerio documentation, with some paraphrasing but no added details.

> What strategies could you employ to compromise the privacy and availability of Bunkered?

The scenerio draws on two characters. One, Bunkered, is a well-heeled network security management firm. Elements from their description will be drawn as necessary, but the general presumption is they are generally an *active* security organization who believes they are implementing best practices. The second, Evil, is an intruder without public identity and limited resources. The general presumption is that the intruder is capable of many technical feats which do not require additional resources (such as cryptographic codebreaking machines or physical access to the Bunkered facilities). The approach of Evil, however, will be summarized by Sun Tzu as a clever fighter.

> *What the ancients called a clever fighter is one who not only wins, but excels in winning with ease. Hence his victories bring him neither reputation for wisdom nor credit for courage. He wins his battles by making no mistakes. Making no mistakes is what establishes the certainty of victory, for it means conquering an enemy that is already defeated. Hence the skillful fighter puts himself into a position which makes defeat impossible, and does not miss the moment for defeating the enemy.* [4:11-14]

Other portions of the scenerio will be introduced as necessary. Having introduced the characters, we present the conflict.

> You have a strong personal animosity towards Bunkered

There are three distinct ways this animosity may be directed. Each provides a rich offensive environment, and so each will be addressed. The first axis of contention is the *personal* nature: are we concerned with the personnel of the organization, or the organization itself.

Personnel concerns may be generated by vendetta or because of a believed arrogance or slight against the attacker or element of the attacker's culture. The attacker may be otherwise motivated against the existance of the organization – as a threat, as a proving ground, or some other motive.

> *No ruler should put troops into the field merely to gratify his own spleen; no general should fight a battle simply out of pique. If it is to your advantage, make a forward move; if not, stay where you are. Anger may in time change to gladness; vexation may be succeeded by content.* [12:18-20]

Sun Tzu seems unambiguous on this point: ego has no place in the realm of strategy. And yet, we may ignore some of these applications – in the assault of Evil, we are responsible for and risk only ourselves. From this, we derive two forms of assault – those on the persons of Bunkered (**1.2**), and those on the Bunkered business.

Within the assault on the business, we face another axis of contention: Time. How long do we wish to engage in the assault on Bunkered, and by what metrics will we consider victory?

> *Move not unless you see an advantage; use not your troops unless there is something to be gained; fight not unless the position is critical. If it is to your advantage, make a forward move; if not, stay where you are.* [12:17,19]

Time can be an effective strategy, and is often within a cracker's toolset. Therefore, strategies **1.2** and **1.4** presume arbitrary amounts of time. Strategy **1.3** reflects a more immediate offensive, with a different objective and payoff.

1.1 Overview of Assault Strategy

> *Do not repeat the tactics which have gained you one victory, but let your methods be regulated by the infinite variety of circumstances. He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called a heaven-born captain.*[6:28,33]

We will not give specific attacks – no sample exploits or direct paths. Through Sun Tzu, we will sculpt a strategy which will give the attacker the disciplines which might permit success against superior strength. Then we will attempt to draw a strategy where the Bunkered defender may have a comparable chance against these strategies.

As the attacker, and as an unknown, we have several advantages which must be maintained. Being unknown, it becomes impossible for Bunkered to adequately anticipate a specific attack.

> *By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided. We can form a single united body, while the enemy must split up into fractions.* [6:13-14]

Therefore, a general principle would be untraceable actions. This means no direct connections from our machines into Bunkered. And it means using alternative connections (*port redirection*, *anonymous dialups with false information to Clueless* for any attacks. As well, behavior should be maintained such that there is no indication of specific targetting - reloading just one specific file on the Bunkered webserver, for example, might be suspicious.

This also guides the motive towards small, well-hidden and well-observed attacks.

1.2 Personnel Assault

Personal privacy of information has continually been reduced in our information-addicted society. This is especially true in the case of technologically sophisticated people. Posts to USENET or mailinglists, from however long ago, continue to be archived and discoverable.

Bunkered may be targetted by collecting as much information as possible about various critical staff members. Obtaining names is easy: anonymous phonecalls for common names or positions, or corporate information sources and reporting. These fall within the realm of social engineering, and is a risk of our information society. Based on the level of access Evil can obtain, the results of personal information can be personally devistating.

Outside the scope of the scenerio, various threats to critical information workers could be destructive to the company (like, if the CTO upon which the company is built leaves) or its availability (system administrators).

1.3 Impatient Assault

Perhaps Evil needs to prove a point and take down Bunkered. There may not be the time, or the motive, to perpetuate a reputation attack (as in **1.4**). This would be to compromise the *availability.*

> *If we wish to fight, the enemy can be forced to an engagement even though he be sheltered behind a high rampart and a deep ditch. All we need do is attack some other place that he will be obliged to relieve.* [6:11]

Unless we are very lucky, it is presumed that the Checkpoint firewall will be secured as bugs are released. Unless we have the resources toward a research program in discovering new bugs in commercial software, we must presume that a single-connection attack will be ineffective.

We may either launch a Distributed Denial of Service (DDoS) attack, or follow Sun Tzu's advice: attack the managed clients. If one was clever enough, this could be temporarily devistating. Consider the following implementation:

- compromise the routers of **Clueless**
- compromise the firewall of **Careless**
- modify careless firewall to block **Bunkered**
- compromise the firewall of an additional **Bunkered** customer
- DoS (*any form*) **Careless** in significant way
- modify **Clueless** routers to interfere with **Bunkered** routing
- as **Bunkered** responds to **Careless**, DoS additional clients

By attacking clients, we engage Bunkered. As Bunkered struggles to fulfill their contractual obligations, their own communications availability is diminished, and the resources they would devote to that are divided between enabling them to relieve Careless and maintaining their own status. As they begin to handle each situation, another of their (previously ignored) customers is attacked. In this way, they are never given an opportunity to implement best practices, and their repair and audit capacities will be compromised in the interest of firefighting.

1.4 Destruction of Trust

The largest vulnerability of Bunkered is its reputation. For trust attacks, time is critical. As the DDoS attacks of Yahoo et al demonstrate, brief incidents rarely reflect poorly on the company. It is generally known that there are immature vandals out there (as anyone who has caught a virus has faced), and no company can really be held liable for massive attacks.

> *The spot where we intend to fight must not be made known; for then the enemy will have to prepare against a possible attack at several different points; and his forces being thus distributed in many direction, the numbers we shall have to face at any given point will be proportionately few.* [6:16]

In the scenerio, we learn that Bunkered has outsourced its webserving to Careless. This is done physically, so interception is impossible.

If we can compromise the Carelesshosting webserver, we can reduce trust in Bunkered through means of false injection. This is done by tampering with some small element of the webpage. Observe how long the response time is for it to be detected and fixed (something minor, like misspelling an executive's name in some report). Ramp up, slowly, through sentance manipulation (paraphrase a sentance, eliminate a sentance). Several options are then possible.

- False News
  Subtly alter and inject additional false news elements to the archives. This will cause the entire dataset to be considered tainted.

- False Advisories
  If **Bunkered** publishes advisories, attempt to emulate and spoof an advisory. Have it appear significant and sincere, and watch the fallout as it is disproved.

- Alter checksum values, binaries
  False, virus-infected or trojan'd binary distribution is a serious offense.

A slow approach is benefitial here, because as a network monitoring organization, it would be considered a serious blackeye if it is discovered that this has been going on "for a long time" undetected.

Another trust manipulation is the disruption and injection of client relationships. If we can monitor email, even at the client-end, we may detect vulnerabilities: do they use encryption or authentication? Does the client *check* authentication marks? If we can inject messages to the client at the mailspool level – or block messages between them – these will cause privacy and availability concerns.

1.5 Defense

> *It is the business of a general to be quiet and thus ensure secrecy; upright and just, and thus maintain order. He must be able to mystify his officers and men by false reports and appearances, and thus keep them in total ignorance. By altering his arrangements and changing his plans, he keeps the enemy without definite knowledge. By shifting his camp and taking circuitous routes, he prevents the enemy from anticipating his purpose.* [11:35-37]

In 1.2, the assault is on the personnel. This will always remain a vulnerability of legitimate enterprise. Therefore, we may draw model from not-completely-legitimate enterprise: underground organizations.

Part of what makes a cracker group distinct is the use of handles as the only identifying characteristics. The FBI has the resources to determine physically mappings between humans and their aliases, but the resource-limited attacker may not.

By adopting aliases within an organization, it may be possible to detect identity probes (consider honeypot and email address spam avoidance techniques as models), as well as reduce information gathering strategies. The less the attacker knows, the more difficult it becomes.

The other is constant vigallence. This is probably part of the business plan, but it must be enforced. This means tripwire checking of anything with which the company is involved in. In the 1.4 case, for example, this means cronjobs which check (both from a known IP and an unknown (Clueless?) IP the validity of the site. Running a frequent diff would alert an operator to any of the small changes, which should cause intense scrutiny of the webserver.

2 Policy

Evil has an inherent advantage.

> *Knowing the place and the time of the coming battle, we may concentrate from the greatest distances in order to fight.* [6:19]

Entropy tells us it is also easier to destroy than to create, and this applies to business processes. However, the legitimate organization has more resources to throw at protection, and the power of governments for those who do bad things.

Policy should reflect that there will be successful attacks. Open disclosure policies, along with rigorous authentication and vigillent monitoring, eliminate many of the risks of trust manipulation.

Humans will always be a weak-link, but this may be offset through enhanced traps (such as pseudonyms for all critical staff, distinct from their past and personal lives).

And finally, commercial vendors (Microsoft, Checkpoint) without reliable histories only make life more difficult for the security conscious.

References

[1] Sun Tzu. *The Art of War*
Source of translation: `http://classics.mit.edu/Tzu/artwar.html`