An Evolutionary Approach to Cyber Security

Carla Marceau
ATC-NY
33 Thornwood Ave. Suite 500
Ithaca, NY 14850
(607) 266-7110
carla@atc-nycorp.com

ABSTRACT

Reducing the risks introduced with large new systems requires rethinking the way we build systems. Today's computer systems are built according to traditional engineering models, which emphasize simplicity and efficiency but which introduce an unacceptable risk of misuse in large-scale systems. We need a new paradigm that results in "messy" systems that evolve through small incremental changes and localized failures.

1. INTRODUCTION

In response to a perceived increase in the threat of terrorist attacks, various measures based on computer technologies such as national identity cards and biometric databases have been proposed. This position statement will consider the United States proposal as an illustrative example. Most software engineers have a good idea of how to build such a system; it requires cards that are hard to counterfeit, a national database of fingerprints or other biometric data, and 24/7 online access from identical fingerprint readers across the country.

Let us admit, for the sake of argument, that such a system can be specified, that biometric technologies can be made to work, and that the large centralized system can be deployed without excessive delay. Such a system still has the disadvantage that it puts everything the bad guys want into one convenient basket. Learning how to counterfeit a single card format enables a malicious person to produce convincing false identities. Breaking into a single database gives access to identifying data about every citizen.

The problem is that our traditional methods of engineering are ill suited to producing the "messy" kinds of system that are resistant to attack. Engineering virtues are oriented toward efficiency; we aim for perspicuousness, economy of means, and the elimination of redundancy. Of course, we add back some local complexity for the sake of fault tolerance and security. However, elegance and simplicity remain essential engineering virtues, and they dominate the overall system design.

I claim that we need to rethink these traditional virtues. I first briefly examine an example of a complex system that has some desirable properties and then consider ways of constructing such systems.

2. A RESILIENT IDENTITY SYSTEM

Consider the Czech identity system as an example. A person in the Czech Republic typically has a driving license, a passport, a birth certificate, and a national identity card. Each identification document serves to identify the bearer in some situations. For driving, the driving license suffices. For very important purposes, such as getting a marriage license, all of them may be required. The various types of identification are supported by independent bureaucracies and separate databases. An important feature of this system is the difficulty of predicting exactly which types of identification will be required; a traffic cop usually asks for a driving license, but can ask for the national identity card as well, especially if there is some reason to be suspicious of a car or driver.

This system is much more complex than the one our hypothetical engineer would have designed. It uses multiple overlapping technologies, stores information in various incompatible databases, and permits inconsistency between the various databases. However, these very vices (from an engineering point of view) help to make the system more resilient.

First, the Czech "system" uses multiple technologies. To gather a lot of disparate information, a thief has to break in not once but several times, each time struggling with a new system and overcoming different defenses. Diverse technologies increase the thief's cost as well his risk of detection. A major violation of confidentiality or integrity would require multiple independent system failures—e.g., a thief breaking into multiple independent databases or foiling multiple biometrics devices.

The points in this and the following section are summarized in tongue-in-cheek morals, each of which contradicts traditional engineering wisdom but contains an important kernel of truth for building national-level survivable systems.

Moral: A*void refactoring.*

Second, the Czech system is compartmentalized, which limits the damage a single attack can inflict. We aren't very good at preventing data theft, including invasion of privacy and identity theft. Why make data theft easier for the bad guys? Spreading data around and compartmentalizing it reduces the expected damage from any single attack.

Moral: *Avoid data concentration and interoperability.*

Third, when mistakes happen—as they inevitably will—the Czech system makes them easier to correct, because it includes

New Security Paradigms Workshop '02, September 23-26, 2002, Virginia Beach, Virginia.
Copyright 2002 ACM ISBN 1-58113-598-X/02/0009 ...$5.00

redundancy, which makes inconsistency possible. Inconsistency is actually a Good Thing, because we can use it as a trouble indicator, just as accountants use inconsistent results on spreadsheets to detect and locate errors. The result is that damage can be repaired and may even be easier to detect.

Moral: *Embrace inconsistency.*

3. SMALL FAILURES ARE BETTER THAN LARGE FAILURES

The Czech identity system began as four independent engineered systems that evolved into a workable amalgam. The key word here is "evolution." To create complex survivable systems of systems, we need an evolutionary approach that encourages small experiments with new technologies; permits but strictly limits the scope of failure in those experiments; encourages the spread of successful technologies and systems; and accepts diversity.

Such a system has two important characteristics. First, it tends to result in "eco-systems" of overlapping systems, as in the Czech model. Second, it uses small failures to weed out the bad or unworkable approaches. Failure is particularly important; the goal is to prefer small failures to large failures.

For example, legislation proposed in 1998 would have required fingerprint information in a uniform format on all state driving licenses. This proposal was widely opposed on political grounds. Technically, a major risk of such a system is that failures would be hard to find and correct. Has an error left your fingerprint associated with a convicted felon? Good luck repairing your reputation. In addition, all databases would be accessible using the same methods—unfortunately, that may be unavoidable in a system that permits drivers' licenses to be used nationally for identification. A third risk is that the system, once mandated, would be tend to be retained forever, once expensive fingerprint-readers have been installed nationwide.

However, consider some alternatives. First, suppose that instead of mandating one technology for all driving licenses, the federal government held a contest every five years for the best state identity system. All states would be strongly encouraged to adopt the winning technology, perhaps in addition to their current techniques. This would be expensive, but it would be more expensive to install a single system nationwide and stay with it forever—especially if it doesn't work well. Alternatively, the federal government could issue an *optional* fingerprint-based identity card, which would essentially compete with driving licenses. For each state, an independent board would decide whether the state license met minimal standards for authentication; if a state's licenses did not, people outside of the state could demand an alternative, such as a passport or the national fingerprint card. Many other combinations are possible.

Whatever improvements are made to an identity system—and America's current system can certainly stand improvement—should be undertaken with failure in mind. Imagine creating a fingerprint-based identity system. After testing, such a system should first be deployed at one or more universities known for their technological prowess, which would use it to guard both grades and money. If the students at Berkeley and MIT can't break the system, it might be ready to deploy on a larger scale, say throughout a (small) state. Technology that has proven itself in one or more states may be mature enough to be adopted at a national level.

Moral: *Build without a plan. Encourage failure.*

4. CONCLUSION

Redundancy, compartmentalization, and the use of multiple technologies are used successfully in engineering for fault tolerance, but they are typically engineered into individual components, rather than emerging as properties of an entire system. Little is known about applying these principles to the security of large systems.

When faced with a crisis, people naturally want a quick fix. However, we (the computer community) are not very good at building systems of systems, and we're not yet very good at security. For these reasons, a "quick" engineering fix would introduce high risks during deployment and would be hard to defend from attacks and maintain in the face of errors. An evolutionary approach will minimize the risk of harm and is more likely to result in a resilient, defensible, and repairable system. We need to learn more about processes that would support such an approach.

5. ACKNOWLEDGEMENT

Many of these ideas were developed during conversations with my colleague David Baca, and they owe a great deal to his insightful observations, especially about the resiliency of complex systems and the particulars of the Czech identity system.