SANDIA REPORT
SAND2014-16805
Unlimited Release
Printed August 2014

Trusting National Security Systems: Issues for National Security Leadership

Mark R. Ackermann

6/13/2014

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation,
a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's
National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2014-16805
Unlimited Release
Printed August 2014

Trusting National Security Systems:

Issues for National Security Leadership

Mark R. Ackermann
National Security and Policy Analysis
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0421

Abstract

Senior leaders rightly expect defense systems to be reliable and experience supports this expectation. However, today's competitive electronics design and manufacturing environment has led to components and software equally sourced by military and commercial entities. These technologies are in the supply chain of Critical Defense Systems. Wide availability permits reduced cost and increased communication, but also opens access to subversion by an Advanced Persistent Threat. Senior leaders must consider including trust as a design discipline. Senior leaders resist focus on trust because its complex, dynamic, and non-data driven. Trust has interdependent elements that place it in the category of a "Wicked Problem," one whose requirements and solutions are always changing. Research for this paper included a review of internal and external literature to understand human responses to trust; wicked problems; the relationship between trust and current technology, quality assurance and production practices; and examples of successful subversions of the past. The paper concludes with how the three principles of trust, prevention, detection, and mitigation, may be implemented, and presents paths for senior management to establish trust and resolve wicked problems.

June 13, 2014

Acknowledgements

This paper would not have been possible without the patience, guidance and senior-level insight, of Dr. Matthew Levinger, Director of the National Security Studies Program at the Elliott School of International Affairs, George Washington University, Washington DC.

Contents

Executive Summary

This study, conducted by the Systems Analysis Group, examines the topic of trust in relation to National Security Systems and presents issues and challenges for senior National Security leadership. The study of trust as a national security concern was commissioned by the Nuclear Weapons Strategic Management Unit and performed between January 2013 and May 2014. This specific report was derived from a paper and coursework completed as part of the Senior Manager's Course in National Security Leadership, taught at the George Washington University, Elliott School of International Affairs as part of the National Security Studies Program. The methodology included an in depth literature review of topics related to trust including wicked problems and approaches to their resolution; security threats, breaches, and methods of protection; and, engineering design and manufacturing principles, techniques and issues.

Today, senior leaders must deal with the effects of intentional changes covertly or clandestinely placed into components and systems. These changes, known as subversions, result in a system appearing to perform as designed, but exhibiting unwanted excursions under certain conditions. These systems cannot be trusted to function as intended. The response to real and potential clandestine attacks is the emergence of what will eventually become a new discipline, one that should be incorporated into government and military systems today. This new discipline is trust.

Trust is a very complex concept with both technical and organizational aspects. Trust cuts across multiple technologies and organizations with extremely complex, and at times uncertain and unknown interdependencies. To prevent unwanted changes in systems, trust programs are essential.

Trust is defined as the justified confidence that a system will function as designed when needed. The justified confidence results from a combination of design intent, testing, and surveillance activities. Design intent assures that the system design minimizes the chances of a clandestine modification that could change system function at a later time and place. Testing requires the system be exercised in conditions that are as close to actual intended use as possible to see if unexpected behavior emerges. Surveillance entails the long-term revisiting of test data and periodic testing to determine if changes in behavior appear.

A trust program includes three main elements: prevention, detection, and mitigation. Continual change must be at the core of a successful trust program. Senior leaders must examine the relative cost and benefit of various approaches to trust and select the one that promises the best return on investment.

The concept of trust and the need for a trust program introduces significant challenges for senior leaders in military and government organizations, and in many cases, commercial enterprises. Trust is a wicked problem. It requires an approach to problem solving that is holistic, system focused, and collaborative.

Acronyms

APT	Advanced Persistent Threat
COTS	Commercial off the Shelf
DOE	Department of Energy
MIL-STD	Military Standard
SNL	Sandia National Laboratories
USB	Universal Serial Bus

1 INTRODUCTION

National security depends upon a myriad of systems and processes. These range from the latest fifth-generation stealth fighters and intelligence collecting satellites to mundane processes for purchasing toilet paper, field rations and office supplies. Many systems and processes experience daily use while others are exercised rarely, or only in times of war. These systems are trusted to function as designed when and where they are required. Although trust implies confidence, the justification for such confidence is unclear.

Gamblers understand past experience and how it relates to games of chance. Stochastic processes function without memory and are both reliable and repeatable. While it is impossible to predict the exact outcome of a specific trial event, the expected average outcome of many trial events can be predicted within certain statistical bounds. Confidence in the outcome of events described by a random process is reasonable and rational. A problem occurs when an event appears to be a random process but is not, and the emotional comfort associated with the event leads to unjustified trust.

Investors deal with events and processes that are statistically random and emotionally driven. These events and processes often include human interaction, which is inherently based on emotion rather than random processes. Prudent investors understand that, for such processes and events, past experience is not indicative of future performance. Any trust in such activities is purely emotional and therefore unwarranted.

Senior leaders largely believe that critical defense systems will function as required in times of conflict. They trust these capabilities based on past experience and knowledge of personnel and physical security systems, and processes. While such trust might seem to be based on reliability and repeatability, it is actually an emotional response based on comfort with past experiences [1].

If the events and processes that senior leaders rely on are entirely random, their trust would be warranted. What would happen if these processes were intentionally altered to appear normal and random, but actually exhibited carefully controlled behaviors? In such a case, the senior leaders' false sense of trust could be exploited by an adversary.

Through clandestine means, systems and processes can be altered, to exhibit carefully controlled and concealed behaviors. These systems might function as intended during times of peace, but would be ineffective in times of crisis. A clandestine attack that alters the function of a system or process is known as subversion. A significant opportunity for an adversary to introduce subversion is through supply chain attack. Other paths exist but require some form of witting or unwitting agent inside the targeted organization. Components, systems, materials, processes, and software can all be subverted. Clearly, subverted systems should not be trusted.

Given that subversion of critical systems and processes is possible, how can senior leaders trust these systems to function when and where required in times of conflict or crisis? The simple answer is that they cannot. Without taking specific actions to establish trust, no basis to trust or not trust these systems exists. The trustworthiness of the systems and processes remains unknown.

Trust is an enduring and complex problem that requires a long-term solution. To help establish justified confidence in systems and processes, senior leaders must establish a grand strategy for trusted systems that will transcend changes in business climate and leadership.

This paper examines the topic of trust for national security systems and presents a discussion of issues and challenges for senior national security leadership. The next section frames the problem, presents relevant background information, includes a basic discussion of trust and wicked problems, and provides examples of subversion. The background information is followed with a brief discussion of three of the more important issues for establishing trust in critical systems: how the approaches for establishing trust are contrary to current trends in design, how these approaches are contrary to current trends in quality manufacturing, and how the very concept of trust forces senior leaders out of their comfort zone. Finally, problems require solutions. The challenge for senior leaders is to work towards solutions for establishing trust. The last section examines these challenges and provides insight into how solutions might be developed.

While trust applies equally to systems and processes, much of this paper concentrates only on systems.

2 BACKGROUND

Trust is defined as the justified confidence that systems will function as designed, when and where they are required. The justified confidence results from a combination of design intent, testing, and surveillance activities. Design intent means that the system was specifically designed to minimize the chances of a clandestine modification that could change system function at some later time and place. Testing requires the system be exercised in conditions that are as close to actual intended use as possible to see if unexpected behavior emerges. Surveillance entails the long-term revisiting of test data and periodic testing to determine if changes in behavior are beginning to appear.

2.1 The Nature of Trust

Trust as a System Property

Trust is a property of a system, much as quality and reliability are system properties. Trust, however, is considerably different from both quality and reliability. A competent adversary will want the targeted system to exhibit its intended design quality so that no suspicions regarding subversion arise. Similarly, the adversary will want the system to be reliable as designed so as not to draw unnecessary attention.

Reliability and trust may appear to have similar goals, the proper function of a system, but the two have significant and fundamental differences. Consider a system designed to have a reliability of 80 percent when used in a crisis. If ten systems were available, one would expect that on average, eight would function as designed. When introducing trust into the situation, the results change significantly. A system with 80 percent reliability and 100 percent trust would produce similar results with an average of eight functional units and two malfunctions, given an initial employment of ten units. If instead, one has only 50 percent trust, there are two possible outcomes with equal probabilities. One outcome would again have eight units function and two fail. The other possible outcome is ten failures. Trust itself is not reliability but is instead a measure of the dependability of the system’s reliability.

Another key difference between reliability and trust is that reliability is based entirely on measured data and mathematical models, while trust will always include an emotional or subjective component [2]. Trusting a system without evidence to justify that trust is a subjective choice that can lead to significant negative consequences. Similarly, undue suspicion regarding a system can lead to mistrust when there exists no rational basis for such mistrust. This, in turn, can lead to erroneous actions to protect the system from a danger that is not present.

Characteristics of Trust

Trust has a number of important characteristics. Understanding these characteristics can help formulate an effective approach to developing trusted systems. The first characteristic is that trust must be evidence-based. It is necessary to have evidence of design intent, and evidence from test and surveillance activities to establish some level of trust. To avoid subjective evaluations, evidence of design intent should include results of positive measures such as independent design reviews and vulnerability assessments.

Trust is transient. Systems that are trusted today cannot automatically be trusted in the future. Over time, an adversary has additional opportunities to obtain access and introduce subversion into a given system. A subversion may be designed for time-delayed activation thereby only being revealed at some point in the future. The transient nature of trust requires that it be continually reestablished through testing and surveillance.

The level of trust placed in a system or process should be proportional to the quantity and quality of trust related evidence and inversely proportional to the consequences of failure in a crisis. High consequence systems require high levels of trust based on a significant quantity of high-quality trust-related evidence.

The Need for Trust

When first introduced to the concept of trust, senior leaders often ask why systems and processes should not be trusted. Past experience suggests that critical systems function mostly as expected in times of crisis. While such confidence may have served senior leaders well in decades past, the world has changed significantly over the intervening years. Today, national economies are largely interconnected and interdependent. Many consumer products benefit from globalized production. Information systems that largely did not exist a quarter century ago are now ubiquitous and highly interconnected, making critical information on sensitive defense systems openly available. Miniaturization of electronic components greatly expands function and capabilities, but also makes it more difficult to verify that unintended features are not present.

Another significant difference today is the emergence of an adversary known as the advanced persistent threat (APT) [3]. This adversary differs from those encountered in the past with technical competence and clandestine capabilities normally associated with the intelligence services of a foreign government. The APT will have significant resources and technical capabilities similar to those of a major research university, national laboratory, or nation state. Finally, the APT is both persistent and patient. The APT might work on a given problem for years because the perceived benefit of success is enormous.

2.2 Trust is a Wicked Problem

Upon further inspection, the intricacies of trust continue to emerge. Trust involves interdependent organizations, processes, policies, technologies and system requirements. Most of these nested interdependencies have both positive and negative feedback mechanisms that interact with other aspects of the system. It is very difficult to make simple changes without significant ripple effects through the entire network.

Trust is best described as a "Wicked Problem." The concept of a wicked problem was first introduced by Rittel in 1973 and was used to describe the difficulties of urban planning [4]. Wicked problems are a class of exceedingly difficult problems that defy traditional linear analytic solutions, and in many cases, defy any solution at all. Lawrence Peter, father of "the Peter Principle," once noted that, "Some problems are so complex that you have to be highly intelligent and well informed just to be undecided about them [5]."

The published literature on wicked problems is rich with various authors providing differing discussions as to what constitutes a wicked problem. A general set of characteristics, although not universally accepted, is discussed below [6].

Wicked Problems are Difficult to Clearly Define

The general nature of the problem is readily grasped, but attempting to decide specifically what fits within the definition of the problem and what lies beyond usually involves conflicting organizational interests, policies and business practices. The list of potential stakeholders is difficult to identify as the problem normally has tentacles that reach beyond well-defined organizational boundaries.

Wicked Problems are Interdependent and Multi-causal

It is difficult to change one part of the problem without unintentionally changing other parts. Various parties have differing requirements that are often in conflict with one another. The cause of the problem is difficult to isolate and often there are multiple factors that converge to result in a single, difficult mess.

Wicked Problems Have no Clear Solution

Simple solutions that are obvious to one stakeholder are almost always in conflict with requirements of another. Solving such problems has been described as attempting to squeeze water in one's hands. No matter how careful the attempt, water ends up squirting out somewhere. Wicked problems have too many loose ends and any solution will leave some, if not many, loose ends unaccounted for.

Attempted solutions often have unintended consequences and lead to new problems. Because the problem and underlying social structure is complex, it is difficult or impossible to comprehend fully the impact of an attempted solution on all stakeholders and organizations involved with the problem. Invariably, some groups are disenfranchised or some equities compromised which can lead to rebellion in one form or another, thereby changing and creating new complexities within the original problem framework.

Wicked Problems are Not Static

Wicked problems evolve even as one attempts solutions. Wicked problems are not static but change over time and also change in response to attempted solutions. This precludes hypothesis testing as the very act of attempting a solution alters the original problem. It is rarely possible to experiment with different approaches in the hope of finding an optimum solution.

Wicked Problems are Socially and Organizationally Complex

Wicked problems almost never reside within a single office or corporate stovepipe. They usually include multiple organizations and disparate stakeholders, each with their own behaviors, norms and cultures. Solutions are often incomplete and frequently result in offending one or more parties involved.

Solutions to Wicked Problem Require Changes in Behavior and Culture

Solutions to wicked problems always include changes in organizational behavior and culture [7]. This is perhaps the most important and defining characteristic of a wicked problem. Changes to behavior and culture are almost impossible for most organizations without the motivation of an existential crisis, and even then, most fail the test. Changes in behavior require addressing issues and organizational values that include status, certainty, autonomy, relatedness and fairness.

Change is by nature threatening, and organizations and individuals often work against change. Senior leaders, however, can implement change so it is viewed as positive and rewarding. In most large organizations, the desired end behavior of any change effort already exists within some subgroup of employees. The key for leaders is to identify the subgroup with the desired behavior and then elevate their status, identifying them as being the model for how the organization can adapt itself to address the perceived external threat [8]. Threats are perceived as negative and individuals instinctively work to distance themselves from the threat. Rewards, on the other hand, tend to draw people in and motivate them to become part of what they perceive to be the in-group [9]. As with any leadership activity, this takes effort, but the results will be achieved more rapidly and will be longer lasting. Rather than threatening values such as status, certainty, autonomy, relatedness and fairness, this alternate approach reinforces those values within select subgroups without threatening the larger population that needs to adapt and change.

Trust as a Wicked Problem

Trust certainly exhibits the key characteristics of a wicked problem. Trust is difficult to define. It is easiest to give examples of what trust is not, but clearly articulating what trust actually is proves difficult with no clear consensus among potential stakeholders. Trust is interdependent, bringing together the disparate cultures of research and development, acquisition, testing, planning, policy and operational execution. No one organization owns the problem and each has its own critical interests that do not always align with those of other stakeholders.

The causes of mistrust are equally difficult to identify. Some are due to our own work patterns, some result from changes in technology, while others are clearly the work of malevolent external actors. With such complexity, there exists no clear path towards establishing trust. Any potential solution will compromise values of various stakeholders and set in motion uncontrolled, unimagined and unintended consequences. The complexity increases as both the problem and the stakeholders evolve in time. Technical solutions to niche problems that exist today might actually introduce vulnerabilities tomorrow. Organizations that had no interest at first might become deeply entrenched in the policy and implementation of solutions in the future. Finally, any attempt to establish and verify trust in systems and processes will require changes to the way people execute their jobs today. This unavoidably requires a change in organizational culture. Change brings with it certain threats to individual values, but if handled correctly, leaders can work to enhance the status, certainty, autonomy, relatedness, and fairness to reward those who adapt and help the organization change.

2.3 Examples of Subversion

For individuals and organizations that have not been the target of a malicious attack, it is difficult to convince them of the need for a trust program. For most people, the concept of an advanced persistent threat (APT) and the idea that someone might be trying to use clandestine means to subvert systems and processes is quite foreign. Most citizens of western societies are open, trusting, and more concerned with day-to-day life than entertaining thoughts of spies attempting to penetrate secure facilities and subvert systems. For such skeptics, the key to understanding the APT is education. The best education is to examine examples of past subversions. Unfortunately, most examples will be highly classified and not available for public review. There are, however, events from recent history that clearly illustrate the threat and the lengths to which adversaries are willing to go to effect subversion. The following four examples are provided to aid the reader in understanding the nature of subversion and the potential impacts.

Component Interception

The first example comes from the former Soviet Union. In 1993, Victor Sheymov wrote the fascinating book, *Tower of Secrets: A Real Life Spy Thriller*, describing a number of sensitive operations carried out by the KGB [10]. One operation involved the modification of cryptographic equipment belonging to a foreign government. The equipment was intercepted and modified while in transit. Subversion of components and systems usually requires some form of physical access. Often, materials can be intercepted while in transit as security is low and the materials are out of sight for an extended period of time. The Soviet caper described below was, however, much more bold and risky.

Country A was sending cryptographic equipment to its embassy in Moscow. To prevent subversion, Country A maintained strict control over everything. All components were made within Country A, including integrated circuits, circuit boards, assemblies and software. The equipment was packaged in crates, locked and secured with tamper resistant and tamper evident seals. The equipment was loaded onto a truck within Country A, then onto a ship belonging to Country A. The truck and ship were continuously accompanied by security agents from Country A. Upon arrival in a Soviet port, the ship was unloaded and the truck driven some distance to the embassy in Moscow. The truck was driven by security agents from Country A and had an escort vehicle from Country A.

At an internal security checkpoint, the escort car and truck awaited clearance to pass through and continue on to Moscow. While the truck was idling at the checkpoint, KGB agents unlocked the back of the truck and got in, riding to the next checkpoint. Inside the truck, they defeated the locks and security seals, removed the electronic assemblies and replaced them with nearly identical units that had a few extra features. Country A never knew that its encoded communications had been compromised. Making matters worse, the United States never knew that Country A's communications were compromised. Often times, information is vulnerable through no fault in process performance.

To execute this attack, the Soviets had to know exactly what lock would be on the truck. They had to know exactly what locks would be inside the truck. They had to be able to defeat and replace the security seals. They also required very detailed knowledge of the circuit boards prior to shipment so they could have modified units ready to install. This event represents an extremely sophisticated and daring attack.

The lesson from this Soviet operation is that equipment completely built and totally controlled by a single organization cannot be trusted. Trust must be justified, based on design intent, testing, and surveillance.

The IBM Selectric

The second example also comes to us courtesy of the Soviets. During the late 1970s and early 1980s, the IBM Selectric typewriter was the instrument of choice for most office correspondence. It was an innovative design that used a single rotating ball to create all characters. The typewriter worked by rotating the ball to the correct position, both vertically and then horizontally, for each character. The ball, about the size of a golf ball, could quickly and easily be replaced to change font or character set.

For the U.S. State Department, the IBM Selectric typewriter was commonly used in foreign missions, consulates and embassies. The typewriters were purchased in the U.S. and then shipped to their destination through various channels, but never with any security as they were not thought to be critical or sensitive items. Cryptographic systems, on the other hand, were shipped through special channels and tightly secured. Rather than working hard to defeat cryptographic algorithms, it is often much easier to simply intercept communications before they are encrypted or after they are decrypted. This is possibly the Soviet motive for attacking the IBM Selectric typewriters.

In 1983, a friendly foreign government intelligence service informed the U.S. that the Soviets had compromised our secure communications [11]. They either did not know precisely how, or were not willing to share that information. Initially the report was not thought credible, but eventually some members of the intelligence community became concerned and convinced President Regan to bring home all electronic equipment from diplomatic stations in the Soviet Union. To prevent the Soviets from learning of the operation, the effort was executed in absolute secrecy. Those not involved with the program were told that equipment moving in and out of the embassy was just part of routine upgrades in capability. The effort was known as Project Gunman. Until recently, it was highly classified.

When the equipment arrived home, small teams of experts spent hours looking over and through everything. Their inspections included x-ray images of all equipment from multiple angles of view. Eventually, a technician noticed something just slightly out of the ordinary in the x-ray image from one typewriter. Initially, it was not known if the discrepancy was due to the Soviets or a modification in system design from IBM. After further investigation, the CIA team discovered that a metal bar known as the comb support had been replaced with a nearly identical bar that also contained batteries, sensors and transmitter equipment.

The bug was found in a total of 16 typewriters. For its day, it was very sophisticated and almost impossible to find. The bug could sense the position of the typewriter ball just before it imprinted a character. This information was stored until eight keystrokes had been completed, after which the data were burst-transmitted to a nearby receiver. It is not known how long the bugs were active, nor what information was typed on the altered units.

The lesson from Gunman is that the U.S. was in the practice of trusting equipment when there was no basis for trust. In the case of the IBM Selectric typewriters, the trust likely resulted from no one worrying about subversion of such a non-critical piece of equipment.

Critical Software

A third example shall be referred to as the FAREWELL operation. During the early 1980s, the French intelligence service had recruited an asset within a part of the Soviet KGB that was responsible for stealing western technology. The French gave their asset the codename FAREWELL. In July 1981, the French president François Mitterrand informed the U.S. what they had learned from FAREWELL [12]. The KGB had a shopping list of western technologies that were critically needed within the Soviet Union. High on the list were weapon related technologies, but also of high importance were technologies for the Soviet oil and gas industry. Rather than play a game of cat and mouse with the KGB and try to prevent them from getting the technologies, the U.S. developed an operation to allow the Soviets to steal information and technology that had been altered.

The Soviets wanted to build a large gas pipeline from Siberia to Europe. Their plan was to sell gas to the west to raise hard currency critically needed to help keep their economy alive. They had purchased most of the equipment and control systems through a combination of legitimate and illicit means, but were unable to obtain the software necessary to automate the system. The Soviets asked the U.S. if they could purchase the software but the request was declined. Undeterred, the Soviets proceeded to steal the software from a company in Canada. Unknown to the Soviets, the software had been modified so that it would operate correctly for a period of time, and then cause damage to the gas infrastructure by producing pressures in excess of what the pipeline could sustain. The result was a massive explosion in the central Soviet landmass. It is claimed that U.S. launch detection satellites observed the explosion and initially thought the event to be a rocket launch [13].

The existence of FAREWELL was declassified during the 1990s. Since then, a number of reports have surfaced claiming that the subversion and resulting pipeline explosion occurred, while other reports deny the sabotage, claiming instead that the pipeline suffered a relatively small explosion due to faulty components. Those who believe the subversion of control software directly resulted in the explosion also suggest that the Soviets were left in a state where they were unable to trust much of anything they had stolen.

Credit Card Readers

The final example presented is much more recent. In 2008, a group of cyber criminals managed to alter the circuitry used in credit card readers used throughout Europe [14]. The perpetrators are believed to be cyber criminals operating out of Pakistan and China. Given the extent of

Chinese government oversight and control, it is entirely possible this activity was known to and at least tacitly accepted by someone in a position of authority within the Chinese government.

For this attack, credit card magnetic strip readers were altered either during production in China, or during shipment. The modifications allowed the readers to send customer account information to electronic addresses identified as being in Lahore, Pakistan. Tens of millions of dollars were eventually removed from a large number of accounts before the operation was discovered and shut down.

The counterfeit readers could be distinguished from genuine readers by their weight, having an extra three to four ounces. Not suspecting subversion, the bogus card readers were installed in machines across Britain, Ireland, Denmark, Germany, and the Netherlands. The technicians had no previous experience with subverted card swipe readers and therefore had no reason to suspect the new readers were anything other than genuine. This is a classic example of linear thinking, where humans tend to believe that the events of tomorrow will largely be similar to those of today, much the same way that events of today are similar to those of yesterday [15]. Citizens of most western societies are simply not conditioned to be suspicious.

3 ISSUES

The introduction of trust as a system concept brings with it numerous implications for national security systems. Before thinking about trust, there was a naïve confidence that systems would work as designed when and where they were required. With the need to contemplate trust and the possibility of subverted systems, it is necessary to consider the possibility that some critical systems will fail precisely when they are required to operate in a crisis. While trust introduces obvious challenges for senior leaders, before exploring these challenges, it is necessary to examine some of the issues that come along with the introduction of trust. The primary issues are that the concept of trust, or stated another way, the need to be suspicious of systems, is contrary to current trends in system design, quality manufacturing, and human nature.

3.1 Trust Runs Contrary to Current Trends in System Design

When considering the trust characteristics of systems, it is necessary to focus on the supply chain as it is necessary to physically alter components or modify software to subvert a system. It is possible to subvert a system while in the design stage, but for the purposes of this paper, the scope of subversion is limited to supply chain attack. When thinking about supply chain security, the common approach and mistake is to examine direct suppliers. Unfortunately, these suppliers are only a tiny portion of the supply chain. To fully secure the supply chain, it is necessary to consider the entire supply network, all the way back to raw materials. Subversion can take place anywhere within this supply network.

Open Design Practices

For the last two decades, with the rise of the “global economy,” manufacturers of commercial products, particularly consumer electronics, have been forced to compete fiercely to gain and maintain market share. This competition is the driving force behind manufacturing and marketing efficiency practices that have significantly contributed to a rise in global standard of living, but also leave systems vulnerable to subversion. Many practices are commonly found in the production of both commercial and military systems, while others are unique to either military or commercial systems. Current practices in commercial system design stress interoperability, plug and play, reuse of proven components and subsystems, and in some cases, open architectures.

Interoperability - Interoperability is the ability of a product from a given manufacturer to operate correctly when interconnected with other products from the same manufacturer, or possibly different manufacturers. The connections can be physical or virtual. The key feature is that the systems exchange and share signals and data of one form or another. Interoperability can be as simple as two hand-held tablets being able to talk with one another, or as complex as the ability of a circuit board from one computer to be removed and inserted into another computer without change of function. A key feature of interoperability is that the interfaces are both known and compatible. This requires that specifications for the interface are known, controlled and available. That which is available for beneficial purposes can also be used for malicious purposes. Interoperability, necessary for commercial systems, introduces vulnerability to subversion.

Plug and Play - Plug and play is a term used to describe how external accessories for personal computers can function properly without the need for the operator to load special software. Plug and play builds on the concepts introduced with interoperability but carries the idea further. The basic interface is well defined. When a new piece of equipment is attached to a computer, the computer and accessory communicate and negotiate the signals and resources that are required. If necessary, the equipment supplies the unique software required for proper function of the accessory.

Plug and play introduces enormous vulnerabilities for information systems but to a lesser degree impacts other systems as well. Most government computer systems are now configured and tightly controlled by network administrators. The systems are designed to recognize most Universal Serial Bus (USB) devices and not allow them to function. This helps prevent introduction of viruses from memory sticks, and helps prevent data loss. The problem is that USB interfaces are open to allow mice, keyboards and printers to function properly. Some with malicious intent have simply reprogrammed memory devices to emulate printers [16]. The computer accepts them as valid plug and play devices and allows the user to print data to the memory much as one would print data to a printer. The computer also allows the device to supply software if needed to function with the fake printer. Plug and play introduces enormous issues for trust.

Reuse of Proven Components, Subsystems and Software - Reuse of proven components, subsystems and software modules is now common within both the military electronics and consumer electronics industries. Modern systems contain enormous amounts of code that is difficult and expensive to produce. The code is easily broken down into functional blocks. For many systems, the basic functional blocks are the same, or very similar. Reuse of software helps amortize the investment over multiple product lines. Similar to software, certain electronic components and sub-assemblies are reused across product lines. A great example is the venerable 8051 microcontroller. This now ancient integrated circuit was introduced decades ago as an early microprocessor. It has found significant use in low-end electronic systems as a microcontroller. Subversion of the 8051 while in production would have resulted in suspect components used in thousands of commercial and military systems over the course of two decades. Reuse of components is necessary from an economic perspective, but it introduces vulnerabilities for systems to be subverted.

Open Architecture - Open architecture is another commercial trend that is both popular and has resulted in significant economic activity. Some manufacturers want to keep their architecture proprietary so they can control their part of the market. Others have found that making the architecture open results in thousands of entrepreneurs developing products that help make the basic system more successful in the marketplace. The military does not like to purchase systems that rely on blackbox, or proprietary equipment. When this occurs, they are forced to purchase support and upgrades through this same manufacturer at elevated prices as there are no competitors. Open architectures allow development of new capabilities at lower costs, but these economic benefits come at the expense of increased opportunities for this openness to be turned against them. The advanced persistent threat (APT) can more easily exploit open architectures and introduce subversions.

3.2 Trust Runs Contrary to Current Trends in Quality Manufacturing

Production Processes

Beyond economically favorable design practices lay economically favorable production processes. Here again we find some approaches that are similar between military and commercial systems and some that are unique. As a general rule, quality products do better in the marketplace than inferior products, but the production definition of quality is often different from what the consumer expects. Quality does not necessarily mean expensive or rugged. Quality systems are those that exhibit very little variation in performance from sample to sample. If production variations can be minimized, it is a simple matter to adjust design and performance for the system to give the end user a consistent and satisfying experience.

Two basic approaches exist to produce systems with minimal variation. One is to put tight specifications on all components and then test the resulting assembly for compliance with performance requirements. Systems passing this test are released to consumers while failing systems are either scrapped or reworked. This is an expensive approach as it does not address the underlying causes of variation.

The second approach is to examine the sensitivity of a system to variations in input materials and parameters, and then tightly control only those that are critical [17]. Once the production process is reliably producing systems that perform within required specifications and with minimal variation, the production process is "locked down" or configuration controlled. No changes are allowed without understanding how they will impact production yield.

Quality Assurance in the Supply Chain

Excellent examples of the second approach in the microelectronics world are the qualified manufacturer list and ISO 9000 certified production processes. These two quality assurance mechanisms are very similar in their underlying approach. ISO 9000 certification provides assurance that the manufacturer has taken steps to minimize variation, and the consumer of those components can use them in higher assemblies without having to screen or test the components. Stated another way, a widespread practice in the production of both military and commercial systems is to trust the vendor’s certification that his parts meet required specifications. This is an excellent place for the APT to attack. The vendor trusts his processes, and the manufacturer of next assemblies trusts the vendor. Since acceptance testing is minimized on both sides of this supplier-vendor relationship, the presence of a competent adversary will likely go unnoticed.

Another growing trend of particular concern for military systems is the use of commercial off the shelf (COTS) components [18]. Half a century ago, the military and NASA were the two largest consumers of electronic components. What they wanted, vendors were all too happy to supply. This resulted in many vendors offering parts that were available in both commercial and military standard (MIL-STD) grade. The military standard parts were subject to additional screening with outliers being sold as commercial grade. Today, the market dynamics have shifted to the point where military electronics are a tiny percentage of the total world market. The military can no longer drive the market. To control costs, they are forced into a greater reliance on COTS components. Since COTS parts are produced beyond the control of the military, there exists the possibility that an APT can execute a supply chain attack and subvert the function of the final military system.

3.3 Distrust Runs Contrary to Human Nature

The concept of trust and the need to be suspicious of systems is difficult for many to accept as it tends to run contrary to basic human nature [19]. By design, social indoctrination, or necessity, most humans in society are relatively trusting of one another. Many social scientists believe that some minimum level of trust is essential for the proper functioning of society [20]. A general tendency is towards what is described as temporal linear thinking. Since nothing bad happened yesterday or the day before, the general trend is for nothing bad to happen, so people inherently accept that nothing bad will happen today or tomorrow. Most people believe that small problems can be fixed before they become large, and spatial linear thinking suggests that big problems have big causes [21]. When bad things do happen, even if they could have been predicted, the general response is one of shock and disbelief. Small failures are quickly rationalized as being anomalies rather than evidence of malicious activity. While it is true that most anomalous outcomes are more or less random, a few are intentional and designed to appear random so that if discovered, they will not result in unwanted suspicion.

The solutions to the trust problem also tend to run counter to basic human nature. In general, the process required to establish trust in systems is to stop trusting them until such trust can be justified. Frequently, people do not want to do this as it is easier to trust.

People also tend to work against efforts to establish trust, both consciously and unconsciously. People are imperfect creatures and tend to make mistakes. Some of these mistakes appear minor but can have major impact when exploited by an APT. An example can be as simple as accidentally typing one's password in place of the user name when trying to log into a company network. Someone watching this would see the failed login followed by a successful login from the same IP address. The observer could quickly see that the first user name looked more like a password and try that with the real user name from the second login attempt. Other human responses are more sinister. In many organizations, change is despised. People who do not like the change will actively or passively work against it. Many long-term employees will simply wait out the new boss. When the boss leaves, the unpopular new policy will leave with him/her.

4 CHALLENGES FOR SENIOR LEADERS

The problem of trust will not solve itself. Senior leaders need to take action. A compounding problem is that the concept of trust is relatively new and poorly understood. Most senior leaders would rather deal with the problems they already know than address something that is new, ill defined, and has no clear solution.

4.1 Aversion to Wicked Problems

Why are senior leaders averse to wicked problems? Large, successful organizations have evolved over time. They have developed business practices that have led to success and in doing so, reinforced themselves [22]. All business and organizations, however, progress through an evolutionary cycle that eventually leads to inefficiencies and bureaucratic inertia. Senior managers become risk-averse, and prefer both quick fixes to difficult problems, and solutions that can be put on autopilot.

Senior leaders are humans and exhibit all the same limitations seen in their staff, such as linear temporal thinking and limited historical memory. Just as random members of the public tend to project yesterday's events onto tomorrow, senior leaders will do the same, even more so if yesterday was routine and uneventful. Thinking about potential changes or catastrophes consumes time and effort that might be better applied to current problems. In addition, people in general tend to have short memories. Unless an occurrence is particularly negative, it will soon fade from memory and not influence current thinking as much as it possibly should. Senior managers exhibit similar traits, which, combined with senior leadership turnover, allow serious problems handled by previous senior leaders to be forgotten.

One of the most vexing problems for senior leaders is assessing the costs and benefits of action on problems with future consequences versus action on current known problems. Trust is one such problem. We know from examples that trust is a serious issue, yet the few known examples of subversion are things that happened to "the other guy," and nothing serious appears to have happened to military systems. Not everything we use has been subverted and trying to find the few that have will be time consuming and expensive. Rather than expend limited resources to address something that might not affect any given organization, even if the potential impact and future cost are assessed to be significant, the leaders will concentrate on current known problems.

The complexity of wicked problems also helps to make the problems difficult for senior leadership. Rarely do wicked problems lie entirely within a single organization. Normally the problems span multiple organizations and business units. There are known and hidden interdependencies that make any modification to the status quo an adventure into the unknown. With cross-organizational dependencies come cross-organizational responsibilities. Addressing the technical cause of a problem might be simple compared to navigating the political landscape to a successful solution. Business units that are composed of multiple stove-piped organizations find wicked problems particularly difficult.

Senior leaders are also at times intimidated by the tendency for wicked problems to change over time in unpredictable ways. Poorly conceived attempts at solutions more often than not make the problem worse. They also introduce new problems. Because the problem changes with each attempted fix, it is rarely possible to learn from one's mistakes and correct a poor solution.

The most difficult part of wicked problems for senior leadership is that solutions always require changes in organizational behavior and culture. Such changes are extremely difficult due to organizational inertia and the tendency of senior leaders to move on after a finite and usually short number of years. Culture change requires seniors to actually lead rather than simply manage. This tends to force them out of their comfort zone. Many people aspire to be senior managers. Few ever succeed at being senior leaders.

An unfortunate truth in much of the corporate world and almost all of government is that the labels of "leader" and "manager" are used interchangeably. Most often, seniors within an organization are referred to as leaders when they are, in fact, only managers. The difference is important, particularly when dealing with change [23]. Managers hold a formal position of status and wield power with the authority of the organization. They have the ability to coerce their staff to accomplish assigned tasks through implied or actual threats. Employees, fearing loss of status, certainty, autonomy and possibly relatedness, conform, whether they agree or not. Leaders have the more difficult task. With no formal position or status, they motivate and persuade individuals to follow some desired course of action by giving their followers status and certainty in the future and a feeling of relatedness. Managers operate in the present and are effective in temporal linear situations. Leaders are necessary for significant and enduring change in organizations.

4.2 Addressing Wicked Problems

Not all is lost. While senior leaders often have a natural aversion to wicked problems, their skill set is reasonably well matched to solving wicked problems. These skills usually include leadership, communication, collaboration, and consensus building, all essentials for tackling wicked problems. Unfortunately, senior leaders often have no formal training and limited experience with wicked problems. Even with experience, every wicked problem is unique. Like any other specialized activity, solving wicked problems requires some training for senior leaders to understand how best to use their skillset.

Approaches to Solving Wicked Problems

The first step is for senior leaders to recognize a wicked problem for what it is. As stated repeatedly above, wicked problems are large and complex issues that span many organizations with interdependent goals and requirements. These are not linear problems that can be addressed with traditional analysis techniques where managers start with a statement of the problem and then work through to a solution.

After realizing that a wicked problem exists, senior leaders need to select an approach that is best suited to that particular problem. The traditional solution approaches are authoritarian, competitive, and collaborative [24]. These are only approaches to solving wicked problems and do not guarantee that a solution will or can be reached. By their very nature, wicked problems are never really solved. They may only be made better or worse.

Authoritarian Approach

The authoritarian approach has the appearance of being the most efficient method to solve a wicked problem [25]. The senior leader will approach the challenge somewhat as a linear problem, but must be aware of the organizational interdependencies and the tendency for unintended consequences. Based on insight and analysis, the leader forces a solution upon the stakeholders. This approach is highly efficient but often ineffective. While the leader can force organizational compliance, the solution lacks "buy in" from those affected. Since it is usually difficult or impossible for a single leader to grasp all the intricacies of the typical wicked problem, the imposed solution will have, at best, a limited impact and eventually the problem will re-emerge in another form.

Competitive Approach

The competitive approach to wicked problems relies on different teams competing to produce a solution to a given wicked problem. A committee is normally formed to review the various proposals and select what is believed to be the best solution. Then, by previous agreement, or royal decree, that solution is imposed upon the organizations and stakeholders. Competitive solutions have the advantage of greater diversity of thought and greater buy in from the stakeholders as they are all involved in the solution. The disadvantage is that the competition takes more time and is therefore not as efficient as the authoritarian solution. In any competition, there are winners and losers and not all will agree with the solution selected and imposed, even if the committee selects the best parts from each proposal reviewed. Competitive solutions are often more effective than authoritarian approaches, but with the stated limitations, they too can be short lived in acceptance and implementation.

Collaborative Approach

The final method for addressing wicked problems is the collaborative approach. This approach should be the easiest and most effective for government organizations as they frequently operate in situations where multiple organizations have interests and there is no clear line of authority. Commercial interests often can sustain more direct control from leadership, but government organizations cannot because different parts of the government are simultaneously involved with the same problem.

For collaborative solutions, the various stakeholders come together to examine the problem and the known interdependencies. With all (or most) players involved, it is also possible for stakeholders to understand the potential costs of inaction. This, at times, helps motivate acceptance of a solution even if it is not optimal for one organization or another. By working together, and exploring common goals and shared values, the stakeholders can move towards identifying objectives and finally developing plans of action. The problem will never completely go away. The collaborative solution will need to be tried and then modified as the wicked problem changes and adapts to the imposed solution. However, through collaboration, it is possible to tame many wicked problems to the point where they are manageable.

The collaborative solution approach is often referred to as holistic [26]. By the collaboration of a large group of stakeholders seeing the big picture and understanding the full extent of a wicked problem, an effective solution can be developed and implemented.

Because wicked problems morph under the stress of an imposed solution, it is necessary for the solution to be resilient, or for the collaborative team to be resilient. Rigid solutions only create additional problems. It is also necessary to understand that the entire problem might not be solved with a given solution formulation. If the critical functions and features of the problem can be addressed and improved, then traditional solution approaches might be more effective on an individual basis for other parts of the wicked problem.

A common difficulty encountered when addressing wicked problems is that the topics themselves tend to defy reasonable attempts at a clear and concise statement of the problem. This often occurs when the senior leader remains focused too closely on one of the components and has failed to step back and examine the larger problem and its environment as a whole. This situation is easily identified when attempts to deal with a problem feel incomplete or unsatisfying. When this is encountered, the senior leader needs to continue to question his assumptions until he arrives at what appears to be the single underlying issue. For many problems with organizational interdependencies, the core of the problem can lie in the political structure rather than the technical aspects of the observed symptoms.

4.3 Principles of Trust

The above discussion of wicked problems and limitations of senior leadership are interesting and important, but do not help organizations address the problem of trust. By its very nature, trust is a wicked, multidisciplinary problem that crosses organizational lines. Based on these characteristics alone, the collaborative approach to problem solving offers the greatest potential for success.

The first step toward a solution is for the known stakeholders to collaborate and determine the organizational extent of the problem and the remaining stakeholders. At first, not all stakeholders will be obvious, requiring the collaborative team to grow over time. As an example, consider the small problem of trust for a single type of integrated circuit used in a critical military system. The first list of stakeholders might include the system designers, users, and maintainers; but this list is incomplete. When this small group begins to explore potential solutions, it will become obvious that other stakeholders such as organizations responsible for procurement, transportation, testing and evaluation need to be included.

The key stakeholders can then collaborate to develop a grand strategy for dealing with the problem. Recall that wicked problems morph over time and organizations and the people in them change over time. It is necessary to have a grand strategy that remains in place to span these changes so future groups and leaders will be committed to collaborative solutions directed towards the same long-term goal. For critical government and military systems, the grand strategy might be to enhance trust in systems through a combination of efforts aimed at increasing the cost, difficulty, and risk for an adversary to attempt subversions; decreasing the likelihood and impact of successful subversions; and increasing the ability to detect and mitigate successful subversions. While this appears to be three separate goals, it is actually a single goal expressed as three individual trust principles. The principles are prevention, detection and mitigation of subversions.

Prevention

Prevention includes a series of positive actions designed to thwart the advanced persistent threat (APT) by reducing the likelihood of successful subversion and increasing the likelihood and cost of being caught. These measures include efforts to reduce the information easily available to the adversary, reduce the possibility of physical access to the system or its supply chain, and reduce the inherent susceptibility of the system to a technical attack.

Detection

Detection is necessary because the best prevention efforts imaginable will not be 100 percent successful. To design resiliency into the trust program, it is necessary to assume that some clandestine activities of the APT will defeat the prevention program. Detection includes a number of positive measures intended to find subversions. The best detection program is systematic, random, and unpredictable. Systematic efforts include planned tests and inspections. Testing should be done under the most realistic conditions possible and include parametric tests, testing to failure as well as failure analysis for components that fail some test. Inspections help to detect subversions that are introduced between production steps, including components and supplies in transit from external suppliers. The aim of an inspection is to make sure that the materials received are the ones that were shipped or released from a previous production step. The question to ask is whether or not the materials received are as expected. Random and unpredictable inspections are necessary as they provide a dynamic defense. Adversaries look for and depend upon predictable processes and practices. Unpredictability brings risk and avoiding detection is generally a high priority for the APT.

While testing is critical for any effective detection program, it is also necessary to test the test systems. One of the easiest ways to put defective units out in the field, be they commercial systems or military hardware, is for the adversary to alter the test systems to control what is accepted. The test system can be designed to pass defective components, fail acceptable components, or even damage systems and report them as passing. A very effective approach to building trust into the test systems is through diversity and redundancy. Whenever possible, multiple test systems should be available, each based on a different design. The specific system used on a given day should be random, and in some cases, one test system can be used to verify the results of another.

Mitigation

Like detection, mitigation is necessary as some subversion will evade both the prevention and detection defense processes. Rather than expect 100% success in prevention and detection, it is necessary to expect that some subversions will be so difficult to detect, that they will sneak past attempts to find them, and the corrupt system will work its way out into daily use. To be resilient, these systems must degrade gracefully if subverted, or if subversions prove fatal to individual units, overall military capability must degrade gracefully. The defective units must be identified rapidly and removed from service.

Critical Components of Success

Two components are critical to the success of any trust program. One is continuous change and the other is resolving inconsistencies. Continuous change keeps the adversary guessing. Stagnant defenses will eventually be understood and evaded, but continuous change introduces uncertainty. The changes need not be expensive or elaborate. Even simple changes are highly effective at introducing uncertainty.

Resolving inconsistencies is also critical for effective trust. Human nature often dismisses inconsistencies as just random error, but some inconsistencies could be subversions. While there are few publically known examples of subversions being discovered, there are many examples of criminal activity being discovered and eventually stopped simply because someone noticed a small detail out of place. It is important to "pull the string" on inconsistencies. Most often they prove to be nothing other than random errors, but on occasion, they will lead to discovery of something that is incorrect.

A significant challenge for senior leaders is to formulate an effective and affordable trust program. If one were to attempt a trust program where everything was suspected, tested to death, verified and tracked under 100 percent positive control, the trust program would become large, bureaucratic and unaffordable. Clearly, not everything can be checked and controlled 100 percent of the time. One approach is to decide what components are critical to the function of a system and protect those, but a clever adversary will figure out how to make a noncritical item into a critical one. A component that is simple and not worth consideration can be the best place for an adversary to attack. The fact is that every component can be attacked, but not every component can be individually checked. This is an illustration of how trust is a wicked problem.

One method to help prevent and detect subversion of simple components is full system testing in the most realistic environments possible. Another approach is for the senior leader to educate his organization on the nature of the APT and encourage subgroups to form teams to collaborate with one another and identify vulnerabilities and solutions. The working level employees are usually the experts on their particular part of the organization. They know best how their work might be subverted, and how to catch subversions. By framing the issue of subversion and the APT as a challenge rather than an existential threat, and by empowering employees to solve the problem, the senior leader rewards contributors with enhanced status and autonomy. The larger workforce will understand their role in the success of the organization and an adversary will have greater difficulty attacking.

Senior leaders will need to examine the relative cost and benefit of various approaches to trust and select the approach that promises the best return on investment. In addition to collaboration with other organizations and stakeholders, it will also be important to include continuous change in the trust approach. The only thing that should remain constant is the commitment to trust. Encouraging individual employees to identify things that need to be changed will encourage them to be part of the solution, rather than allowing change to be perceived as a threat to their existence.

4.4 An Existence Proof for Trust

As an example of an effective trust program, one should consider the personnel security system put in place for special military and intelligence programs. While there have been a small number of spectacular failures, such as the Edward Snowden affair, Private Bradley Manning, Aldrich Ames, and Robert Hansen, the process does work effectively in most cases. When breaches are discovered, they are quickly dealt with by isolating the individuals in question and mitigating the damage to the extent possible.

The first part of personnel security is prevention. Individuals nominated for security clearances are subjected to background investigations, and interviews with security professionals trained to watch for suspicious and evasive behavior. The purpose is to screen out individuals that initially appear to be poorly suited for positions of trust.

After individuals pass background checks and are granted security clearances, the next part of the personnel security system is to detect bad actors. The system assumes that no matter how effective their initial screening procedures are, some unsuitable individuals will be granted clearances. Even for individuals who are initially trustworthy, changes in life situations can lead to some people becoming unsuitable for clearances. Detection processes are put in place to find these bad actors as quickly as possible.

Once security problems are identified, the mitigation phase begins. The individuals are isolated both socially (within secure communities) and electronically while their case is investigated. Many times the problems are resolved and the individuals are returned to a cleared status to resume their work. Other times, the individuals prove unsuitable to continue in positions of trust and are permanently removed from the secure community. Following such incidents, damage assessments are conducted and changes in the security system are implemented if necessary.

Continuous change is essential for any trust program. Personnel security is no exception. In recent years, the emergence of extremely high-density memory devices for electronic information systems has made personnel security exceptionally difficult. Personnel security programs expect a small number of bad actors. In the past, these individuals could only cause limited damage. Today, lone wolf bad actors can quickly steal vast quantities of sensitive information. System administrators are perhaps the most dangerous individuals within any secure community. They generally have access to all information and the ability to modify the configuration of the electronic information system for necessary official purposes. Unfortunately, these individuals can also modify the system for nefarious purposes. To adapt to changes in the threat, the personnel security system must change. The same is true for any trust program. Continuous change is essential.

5 SUMMARY

Following World War II, the world saw the development of a robust electronics industry. At first systems and products were somewhat unreliable and exhibited random variations in performance. Over time, the concepts of quality and reliability gained acceptance and were eventually embraced as valid technical and management disciplines within the industry.

Today, senior leaders must deal with the effects of intentional changes covertly or clandestinely placed into components and systems. These changes are known as subversions. They result in a system appearing to perform as designed, but exhibiting unwanted excursions under certain conditions. These systems cannot be trusted to function as intended. The response to real and potential clandestine attacks is the emergence of what will eventually become a new discipline, one that should be incorporated into government and military systems today. This new discipline is trust.

Trust turns out to be a very complex problem with both technical and organizational aspects. Trust cuts across multiple technologies and multiple organizations with extremely complex, and at times uncertain and unknown interdependencies. To prevent unwanted changes in systems, trust programs become essential.

The concept of trust and the need for a trust program introduces significant challenges for senior leaders in military and government organizations, and in many cases, commercial enterprises. Trust is a wicked problem. It requires an approach to problem solving that is holistic, system focused, and collaborative.

References

1. B. Misztal, *Trust in Modern Societies: The Search for the Bases of Social Order* (Cambridge, UK: Polity Press, 1996).
2. P. O'Connor, *Practical Reliability Engineering* (West Sussex, UK: John Wiley & Sons, Ltd., 2012).
3. E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* (Waltham, MA: Elsevier, 2013).
4. H.W.J. Rittel, "Dilemmas in a general theory of planning," *Policy Sciences* 4 (1973): 155-169.
5. J. Conklin, *Dialogue Mapping: Building Shared Understanding of Wicked Problems* (West Sussex, UK: John Wiley & Sons, 2006).
6. Tackling Wicked Problems, A Public Policy Perspective (Commonwealth of Australia: Australian Public Services Commission, 2007).
7. M. Gray and R. A. Gill, "Tackling 'Wicked' Problems Holistically with Institutionalist Policymaking," *in Institutional Analysis and Praxis: The Social Fabric Matrix Approach*, ed. T. Natarajan and S. T. Fullwiler (New York, NY: Springer, 2009): 87-102.
8. D. Ward, Changing cultures without burning platforms, *CIO Network*, 29 April 2014, http://www.forbes.com/sites/ciocentral, accessed May 2014.
9. D. Rock, *Your Brain at Work: Strategies for Overcoming Distraction, Regaining Focus, and Working Smarter all Day Long* (New York, NY: HarperCollins, 2009).
10. V. Sheymov, *Tower of Secrets: A Real Life Spy Thriller* (Annapolis, MD: Naval Institute Press, 1993).
11. S. A. Maneki, Learning from the Enemy: The GUNMAN Project, National Security Agency (2012). http://www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/publications/Learning_From_the_Enemy_The_GUNMAN_Project.pdf.
12. F. Castro, "Deliberate Lies, Strange Deaths and Aggression to the World Economy," *Center for Research on Globalization*, September 23, 2007. http://www.globalresearch.ca/deliberate-lies-strange-deaths-and -aggression-to-the-world-economy/6861.
13. M. French, "Tech sabotage during the Cold War," *FCW The Business of Federal Technology*, April 26, 2004.
14. A. Modine, "Organized crime tampers with European card swipe devices, Customer data beamed overseas," *The Register*, 10 October 2008, http://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/, accessed March 31, 2014.
15. S.A. Umpleby, "The Financial Crises: How Social Scientists Need to Change Their Thinking," George Washington University School of Business, 14 January 2010.
16. A. Crenshaw, "Plug and Prey: Malicious USB Devices," presented at ShmooCon 2011.
17. M.S. Phadke, *Quality Engineering Using Robust Design*, (Englewood Cliffs, NJ: Prentice Hall, 1989).
18. P.R. Popick, "Requirements Challenges in Addressing Malicious Supply Chain Threats," *INCOSE*, Volume 16 Issue 2, July 26 2013.
19. Misztal, *Trust in Modern Societies*.

20. K.S. Cook, *Trust in Society,* (New York, NY: Russell Sage Foundation Publications, March 2003).
21. A. Boin, "The Crisis Approach," in the *Handbook of Disaster Research*, ed. H. Rodriguez, E. L. Quarantelli, R. R. Dynes (New York, NY: Springer, 2007): 42-54.
22. J. A. Belasco, *Teaching the Elephant to Dance: The Manager's Guide to Empowering Change* (New York, NY: Plume, 1991).
23. "Leadership vs. management," Diffen.com, http://www.Diffen.com/difference/Leadership_vs_Management, accessed May 2014.
24. "Tackling Wicked Problems" (Commonwealth of Australia).
25. N. C. Roberts, "Coping with Wicked Problems," Naval Postgraduate School, Monterey, California, Department of Strategic Management Working Paper (2000).
26. M. Gray, "Tackling 'Wicked' Problems Holistically (Springer).

Distribution

External Distribution:

1 Dr. Donald L. Cook (1 electronic copy)
National Nuclear Security Administration

2 Dr. Matthew Levinger (1 electronic copy and 1 paper copy)
Elliott School of International Affairs
1957 E Street, N.W., Room 605 K
Washington DC 20052

2 Mrs. Karen Notch (1 electronic copy and 1 paper copy)
Elliott School of International Affairs
1957 E Street, N.W., Room 605 K, Suite 601
Washington DC 20052

Internal Distribution:

1	MS0127	Susan Howarth	0248 (1 electronic copy)
2	MS0421	Group 0240 Library	0240 (1 electronic copy and 1 paper copy)
2	MS0421	Mark R. Ackermann	0245 (1 electronic copy and 1 paper copy)
1	MS0421	Russell D. Skocypec	0240 (1 electronic copy)
1	MS0134	Arthur L. Hale	0500 (1 electronic copy)
1	MS0134	John A. Larson	0500 (1 electronic copy)
1	MS0340	Joseph Morreale	2243 (1 electronic copy)
1	MS0127	David L. Kitterman	0254 (1 electronic copy)
1	MS0134	John R. Fellerhoff	0200 (1 electronic copy)
1	MS0104	Jerry L. McDowell	0002 (1 electronic copy)
1	MS1209	James L. Novak	5950 (1 electronic copy)
1	MS0899	RIM Reports Management	9532 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories