This article is part of the IEEE Reliability Society 2007 Annual Technology Report.

Software Trust

Jeffry Voas
Email: j.voas@ieee.org

The field of computer security is basically divided into two areas of specialty: (1) physical (or what is often called perimeter security), and (2) software security, a newly evolving discipline that takes the viewpoint that in a networked world, where the software allows the connections to communicate, that the application, firewall, encryption, and operating system software is our largest vulnerability. For example, application software can contain malicious code, and operating system software can be fooled into allowing people to access resources that they should not be allowed to do. And of course there is virus and worm software functionality to contend with (we'll get more into that later).

Statistics indicate that most intrusions into computer systems are started by "insiders", i.e., people in an organization that already have some physical access to the systems. That has fostered the emerging field of biometrics, which tries to match physical characteristics of people with the level of access into the system that they should have. And this trend will continue, as more and more sophisticated identification technologies come online.

However, as we said, these attacks are mainly done by persons that are known to the organization under attack. A possibly greater looming threat is the result of software vulnerabilities. A classic example is simply the poor programming practice in the C language that allows buffers to be overflowed, via the string processing facilities that the C language provides (such as strcpy()). When programmers fail to make sure that these buffers cannot be overflowed, that allows malicious data (code instructions) to be pushed onto the operating system's stack of future instructions to be executed, and that means that the operating system will then execute the malicious code. For example, it would be possible to push a small set of machine level instructions into a filled buffer, forcing the original instructions to be "pushed away", and then the bad instructions are the functionality that the operating system performs. While this might seem like a simple programmer error, it really borders on negligence, because every programming course teaches students to handle issues related to type safety very carefully. Fortunately, newer languages like JAVA that are interpreted (instead of compiled) offer programmers much help here with a lot of behind the scenes internal type safety and checking). And so over time, some of these bad habits have the potential to become extinct.

One last point to make here deals with encryption. Encryption is vital for data that needs to be transferred from location to location in a secure and private manner. Imagine how the web and internet would have pretty much fizzled had individuals and companies not been able to transfer merchandise orders and emails securely. However while it is true that encryption is great for data transfers, that data still sits on the ends in the databases and computers. Therefore encryption is considered only useful for "point to point" security, and relatively useless for the data is stored on a machine. That then is where a hacker or insider has the best chance of breaking down the efforts of the best encryption, i.e., don't waste your time sniffing encrypted data that is being transferred. It is just too hard. Instead, find a buffer in the OS that can be overflowed. Therefore the commonly heard argument that encryption is the key jewel to successfully achieving security is flawed. It is only one of many jewels that are necessary.

And so today in 2007, the majority of research deals with setting up appropriate security policies, using proper encryption algorithms, employing biometrics, and enormous amounts of monitoring the system (for known virus signatures and patterns) as it executes in order to detect abnormal behavior. And I expect that these will remain the key approaches for years to come. However after having just restated what I wrote in this report in 2003, here are some new areas to consider: (1) the product model for software is gone; software is a service, and now the security of services is a huge challenge, since services are treated differently than software because of their publish/subscribe models, (2) a better understanding between vulnerabilities, exploits, and threats has been occurring since 2003 (although these terms are still misused continuously), (3) the degree of interoperability between subsystems has clearly increased, causing much difficulty in determining which exploit can be combined with a vulnerability to cause the possibility of a threat, and (4) a very new field of study that looks into catastrophic events termed “cyber-pandemics” is now in our vocabulary. I’ll now say a few words about the fourth one as I find it the most challenging.

Cyberspace has become the nervous system of our nation's critical infrastructure. It functions as the information and decision and control system for the operations of our public and private institutions in agriculture, food, water, power, public health, emergency services, government, defense industrial base, transportation, banking and finance, and postal and shipping. As a dynamic system, cyberspace has evolved over time as hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that enable our critical infrastructures to support societal functions. Hence, robustness and stability have not been designed in at the system level. The inherent instabilities in the resulting system of systems can be exploited to cause and propagate blackouts in the critical national infrastructures and in turn generate what is known as the *butterfly effect* in the societal functions that are supported.[1]

Each critical infrastructure industry sector is dependent on other industry sectors. The interdependence of electric power, telecommunications, energy, financial, transportation, emergency services, water, food, and so forth is exacerbated by the embedded electronic devices relied on to provide critical controls. Electric power and telecommunications stand out as critical dependencies for all industry sectors and require special preparation and protection measures.

The objectives of studying the idea of cyber-pandemics are: (i) identify, understand and characterize the inherent vulnerabilities in our cyber infrastructure which may cause debilitating impact on essential societal functions and (ii) instrument effective countermeasures at critical points in the societal systems to mitigate the debilitating effects. An example is the Banking System of the nation and its interactive dynamics with the components of the cyber infrastructure. Can the known and well understood vulnerabilities in individual components of the cyber infrastructure be exploited to cause a perfect storm in Banking? The focus here would be in understanding and mitigating the brittleness of the nation's Banking system, not the triggering individual faults in cyber components. Pathological system behaviors in incidents like the failure of the electric power infrastructure in Western United States in the summer of 1996 emerge as a consequence of the dynamics of interactions between linked processes and are not adequately explained by individual faults or failures. Based on their brittleness, aggregated system behaviors may range from strict order to chaos with great sensitivity to initial conditions.

In banking and finance, the financial services industry depends on a network of systems that process instruments of monetary value in the form of deposits, loans, funds transfer, savings, and other financial transactions. The network is composed of banks, other depository institutions, and the Federal Reserve System, as well as underwriters, brokerages, and mutual funds. In addition there are industry utilities including the New York Stock Exchange (NYSE), the Automated Clearing House (ACH), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT) as well as underlying third party electronic processing services.[2]

The Interagency Paper[3] pinpoints clearing and settlement systems as the most critical business operations at risk for financial markets and the disruptions of clearing and settlement processes would have an immediate systemic effect on critical financial markets. The use of the term “systemic risk” is based on the international definition of systemic risk in payments and settlement systems.[4]

The Federal Reserve Board specified that the following functions are critical to the operation and liquidity of banks and stability of financial markets and require same day recovery:

1. Large–value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), Depository Trust Clearinghouse Corporation (DTCC), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
2. Automated clearinghouse (ACH) operators
3. Key clearing and settlement utilities
4. Treasury automated auction and processing system
5. Large-dollar participants of these systems and utilities

The financial sector depends on maintaining the trust of the banking community and the banking public. In large measure this trust is maintained through the transparency and verification inherent in exchanges. Without this trust the banking system itself risks anarchy. Under what circumstances might trust in the banking system be tested and stressed? At the close of each business day, it is the expectation and practice of the banking community that the banking ledgers of branch offices be reconciled and balanced to the penny and that securities and trading firms create a daily P&L. Under what circumstances of use might the banking ledgers be thrown out of balance impacting the daily closing and settlement process… and the next day opening? More specifically what is the least Physical and Cyber Security exploit capable of impacting next day closing? Overall, the stock exchanges and their associated clearinghouses have performed due diligence and taken the steps necessary to ensure the resilience of their operations. In addition alternate trading systems like Island and Instinet only increase that resilience and even possess the capacity in computation, data storage, and communication bandwidth to sustain normal operations.

However, weaknesses may still exist in the banking and finance sector where trust is not buttressed by verification. Specifically, there are a wide variety of credit derivative products based on an underlying bond instrument from which the trader creates products with option/future characteristics. Unlike stocks, credit derivatives do not operate within the structure of an exchange. Instead transactions are consummated between pairs of traders who effectively set the price of a transaction. Consequently, credit derivatives lack transparency. If trading in credit derivatives were disrupted or trust in the market lost, prices would go down forcing banks to increase reserves to cover the losses. Hedge funds are major participants in the credit derivatives market and do business with Chase Manhattan Bank, CitiBank, Goldman Sachs, and Credit Suisse First Boston. For a calamity to occur it would need to involve multiple participants. Features of an attack that might exploit the absence of transparency include:

1. The operation appears to function properly following a successful attack.
2. Essential data is lost, contaminated, compromised, thought to be incorrect, or not known to be correct, resulting in a loss of confidence.
3. An insider trader launches an attack for profit.
4. The attack is accompanied by a rumor propagated rapidly and widely by a communications tool like a Bloomberg.
5. Backup systems are disabled without detection prior to the primary attack.

In summary, our well being depends on the harmonious cooperation and resilient operation of the nation's critical infrastructure. However, a stovepipe culture of independent silos among these sectors has grown up and is being tolerated. This has resulted in a variety of cultural, technological, and political factors that are positioning the critical infrastructure for failure and calamitous societal impact. This joint vulnerability concretely expresses itself through technology. Here dependence on software has progressed to the point where "software is now the critical infrastructure within the critical infrastructure."[5]

Over time, each industry sector and its system of operation have increased its interaction and interdependence on other sectors until now the critical infrastructure has become a system of systems. While much is known about reasoning about systems and obtaining intellectual control applying arguments of completeness, correctness, and consistency, not enough is known about systems of systems and designing the mechanisms for their operational control and selective actuation during crisis.

The key questions to address in cyber-pandemic studies are:

(1) To what extent does this vulnerability act like stored kinetic energy awaiting the triggering event that could unleash cascading and propagating effects with societal impact?
(2) What industry sectors stand ready to facilitate a national crisis?
(3) Could the triggering event come in the form of a coordinated Cyber Security and physical attack threat?
(4) What tools are needed to prevent this crisis?
(5) Can a Cyber Security Perfect Storm be triggered by a single fast moving attack? Or does it take a carefully coordinated attack scenario? In any event, what tactics offer the best protection? More specifically, what is the least set of supervisory control operations best able to sustain a system of harmoniously cooperating distributed processes?
(6) To what extent is this set of operations currently embedded in the nation's critical infrastructure?
(7) What stepwise improvements are indicated to elevate that protection to a minimally acceptable state?

For information on cyber-pandemics, contact Jeffrey Voas at j.voas@ieee.org

References:

[1] K. Mainzer, " Philosophical Foundations of Nonlinear Complex Systems" Interdisciplinary Approach to Complex Dynamical Systems, Haken and Mikhailov (ed), Springer Verlag, 1993
[2] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report, 2004
[3]The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, "Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System", September 5, 2002

[4] Committee on Payment and Settlement Systems, Bank for International Settlements, “A Glossary of Terms in Payment and Settlement Systems”, 2001

[5]"Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness", Center for National Software Studies, 29 April 2005, http://www.CNsoftware.org