A New Approach to Nuclear Computer Security

By George Chamales

The current, attack-centric approach to computer security is incapable of adequately defending nuclear facilities. This paper introduces a new approach, vulnerability-centric security, which enables nuclear facility operators to prevent successful cyber-attacks while enhancing the day-to-day operation of their systems.

Understanding the Challenge

Nuclear facilities responsible for power generation, enrichment and storage are complex computing environments comprised of hundreds to thousands of individual devices. Those devices, and the computer systems that manage them, are built from a combination of common, off-the-shelf computing technologies and custom, one-of-a-kind hardware, software and networking protocols. The only commonality between these facilities is that a large number of their critical systems tend to be built on legacy technologies.

The reliance on legacy technology is understandable: changing complex systems is a complex undertaking. When an update is necessary, facility operators must tackle a long list of challenges that include working with tight margins and small budgets, maintaining compatibility with one-of-a-kind technologies (sometimes from companies that no longer exist), meeting regulatory requirements and limiting service interruption all while ensuring safe operation before, during and after the change is made. These challenges create significant hurdles when trying to keep pace with the fast-moving world of computer attacks and many facilities struggle to keep up.

The difficulty of keeping up does not excuse nuclear facility operators from maintaining a strong defense; however, criticism of nuclear facility security tends to include an inaccurate assumption regarding what system operators should do to defend themselves.

The assumption is: if nuclear facility operators used standard cyber-security technologies, they would be protected from cyber-attacks.

That is not true.

The current approach to computer security is based on an ad hoc collection of tools that attempt to detect and block cyber-attacks. These tools fail when new attacks are created, and new attacks are being created at an increasingly fast pace. As a result,

nuclear facilities will remain at the mercy of attackers and new attacks that bypass even the most up-to-date attack-centric defenses.
Effectively defending nuclear facilities requires approaching security from a different angle: *preventing successful attacks by proactively addressing computer vulnerabilities*. This vulnerability-centric security approach is based on three fundamental principles that guide how security is selected, deployed and managed:

1. Increase security by decreasing vulnerabilities.
2. Decrease vulnerabilities using deterministic systems.
3. Security should enhance operations.

Many of the technologies necessary to implement vulnerability-centric security are available today, and additional capabilities are under active development. The appendix describes several of these technologies and how they can be applied to nuclear facilities.

The following sections discuss the shortcomings of the attack-centric security approach, followed by an introduction to vulnerability-centric security, its underlying principles and strategies that can be applied to nuclear facilities.

The Shortcomings of Attack-Centric Security

Most of today's computer security technologies were originally built in the late 1980's in an attempt to stop the first waves of cyber attacks. These attacks, made possible in part by the rise of computer networking, created an attacker-driven, attack-centric pattern in computer security: new attacks bypass existing defenses, new defenses are put in place to stop those attacks, and the cycle repeats.

As a result, the evolution of modern computer security technology can be presented as a series of defender reactions:

- Computers are attacked across newly-formed global networks, so firewalls are put in place to block remote access.

- Firewalls fail to stop viruses, delivered inside email or on portable disk drives, so anti-virus programs are built and installed on computers.

- Anti-virus software fails to stop new viruses, worms and other novel exploits, so intrusion detection systems are deployed on internal networks to raise alerts when computers are compromised.

- Alerts from intrusion detection systems do not stop successful attacks, leading to a series of incremental derivations of existing technologies (e.g., host-based firewalls, host-based intrusion detection, and network-based anti-virus) along with the proliferation of penetration testing services - teams of ethical hackers who charge top dollar to point out weaknesses in organizations' cyber-defense.

The attacker-action, defender-reaction cycle has important ramifications for the security of nuclear facilities, where the constant evolution of new attacks forces defenders to constantly update their defenses. The reactionary approach is incompatible with the slow-moving upgrade cycles at nuclear facilities. Facility operators who have managed to install attack-centric security technologies are justifiably leery of the unintentional consequences of new security updates - poorly written anti-virus updates periodically incapacitate the computers they are installed on and the security products themselves may contain exploitable vulnerabilities.

Nuclear facility operators are not the only ones who struggle with the constant need to update their defenses. By the early 2010's, deploying security technologies had become so complex that the security industry writ large developed a new class of product to help organizations make sense of the disparate configurations, updates, warnings and alerts generated by their numerous security products. The rise of these products, named Security Information Event Management systems (SIEMs), marked an important turning point: from the security industry's perspective, security incidents were no longer something to be stopped—they were something to be "managed."

The focus on incident response is justifiable in situations where the consequences of a cyber-attack are strictly monetary. In that context, the money spent on incident response technology appears to pay for itself: when attack-centric security technologies fail, incident response “saves” organizations money because they lose less of it and the remaining losses, which regularly exceed millions of dollars, can be written off as a cost of doing business.

Nuclear facilities do not have the luxury of writing-off cyber-attacks because the potential consequences of a failure are not just financial, they could be physical. Successful attacks can destroy mission-critical machinery, disrupt vital services, and cost people their lives. Attacks which result in the loss of weapons-usable nuclear material or a radiological release would be particularly dangerous. In this context, depending on ineffective security technologies and, when they fail, hoping for an efficient response is not a tenable position. When it comes to nuclear computer security - if you're responding, you're losing.

Nuclear facilities are not the only industry on the losing-end of attack-centric security – all critical infrastructure facilities and corporate networks are in a similar position. The shortcomings of the current, attack-centric approach to computer security stem from tackling the problem of insecurity from the wrong angle: focusing on attacks instead of the vulnerabilities those attacks exploit.

A New Approach: Vulnerability-Centric Security

A new approach to computer security is needed, one that is based on sound principles and technologies that can be used to construct effective defenses. The vulnerability-centric security approach seeks to address the root cause of system insecurity – system vulnerabilities – and creates the opportunity for security to be more than a "necessary evil". Security can be a net-positive for operations.

Vulnerability-centric security is based on three fundamental principles:

1. **Increase security by decreasing vulnerabilities**: Facility operators focus on addressing a limited set of exploitable vulnerabilities in their systems instead of the ever-increasing number of attacks. Eliminating a vulnerability eliminates all attacks against that vulnerability.

2. **Decrease vulnerabilities using deterministic systems**: Facility operators decrease vulnerabilities in their systems by applying tools and strategies that ensure their systems do only what they are supposed to do, instead of deploying expensive, hard-to-manage, attack-detection technologies.

3. **Security should enhance operations**: Facility operators manage their own defenses using tools and techniques that increase their system's reliability on a day-to-day basis, instead of requiring dedicated security technologies that are only useful when under attack.

These principles serve as both a heuristic for evaluating the effectiveness of security controls and as a foundation on which to build more specialized defensive strategies. The following sections describe each of these principles along with strategies (derived from those principles) that can be applied to nuclear facilities.

Principle 1: Increase Security by Decreasing Vulnerabilities

Eliminating a vulnerability prevents all present and future attacks against that vulnerability. This is particularly important in a world where computer viruses and other exploits mutate in order to avoid detection. As a result, an anti-virus program may be capable of detecting permutation 1 - 17 of a virus, but fails to stop permutations 18 - 200 (all of which may already be in use by attackers). By finding and eliminating vulnerabilities, it becomes possible to successfully stop every permutation of the attacks which target those vulnerabilities.

The most common vulnerability elimination approach is computer software patching, often seen in the form of critical security updates. While patching can close exploitable vulnerabilities, the process has significant limitations. Many software updates are only created after a vulnerability has been found and exploited. Even if the vulnerability was kept quiet, attackers can reverse-engineer the security patch to identify the original vulnerability, allowing them to craft attacks against organizations with unpatched systems, such as slow-to-upgrade operational environments within nuclear facilities. In addition, program patches may have unintended side-effects that cause them to accidentally break critical system functionality. More fundamentally, reliance on the patching process assumes that the vulnerable software is still supported by the manufacturer and that the manufacturer is still in business – two assumptions that cannot always be made for legacy systems run by nuclear facility operators.

Successfully increasing security requires the ability to eliminate vulnerabilities without knowing where they are and without relying on system manufacturers. The following are three complementary strategies:

- **Remove Unnecessary Functionality**: Identifying and disabling unnecessary application functionality eliminates the risk that vulnerabilities in that functionality can be exploited. This approach does not necessarily require any new technology. For example, removing an embedded device's unused administrative webserver protects against current and future vulnerabilities in that webserver. As an operational benefit, removing unnecessary functionality during design and testing makes systems easier to manage (since there's less functionality to deal with) and helps streamline the deployment process for system upgrades (since updates to the removed functionality do not need to be tested and verified).

- **Segment Software Components**: Segmenting software limits programs to only access the computing resources they need (processor, memory, disk, network, etc.) to perform their function. Running applications in a software-defined sandbox or on virtualized hardware can prevent attackers from using a compromised application to access and attack other programs or networked devices the computer is connected to. For facility operators, application isolation enables component-by-component testing and upgrades while limiting the impact that attacks and non-malicious program crashes can have on other programs running on the same system.

- **Integrate Security Functionality**: Facility operators can proactively integrate security into their software. These processes include security scanning tools that search through programs to identify unknown vulnerabilities and security instrumentation technologies that add security features to existing programs. The added security features may include the ability to disable unnecessary functionality, segment software components and enable advanced security monitoring and alerts. Manufacturers can use scanning and instrumentation to prevent software bugs during development and facility operators can leverage these tools during their testing and staging processes. When the instrumented programs are placed in production, integrated security functionality can prevent successful attacks by eliminating vulnerabilities and prevent previously unknown faults from causing applications to crash.

Deploying vulnerability-centric security protections on production systems creates an opportunity to detect and address systems that were compromised prior to deploying the new security protections. This is made possible by simultaneously increasing an attacker's risk of detection while decreasing their opportunities to act. For example, removing unnecessary functionality can eliminate hiding spots used by attackers already inside a system. Segmenting components can mitigate some of the threats from supply chain compromises, eliminate attackers' persistent access to computing resources as well as detect and block hidden communications between compromised programs. Security instrumentation extends these benefits into the programs themselves, creating more opportunities to prevent, detect and alert on malicious manipulation of programs at both the vendor and operational level.

Increasing security by decreasing vulnerabilities does require that these new capabilities be evaluated, tested and deployed. These short-run impacts on systems and personnel are offset by the long-run benefits: the vulnerability reduction process simplifies systems (both programs and processes) making them easier to understand, use, manage and maintain. The process of reduction and simplification is essential to addressing a root cause of system insecurity: unanticipated system behavior.

Principle 2: Decrease Vulnerabilities with Deterministic Systems

A well-built deterministic system is one that does exactly what it is supposed to do and nothing else. Early control systems were built using a combination of manual processes and deterministic computing devices. These early devices, many of which were custom-built from hundreds of electrical components connected by thousands of meticulously hand-wound wires, could be verified for functional correctness using a combination of mechanical testing and mathematical analysis. The deterministic nature of these systems made them extremely reliable: they could operate continuously for years without any intervention and, even when they failed, they were designed to fail safely.

Over time, these hardwired devices have been replaced by inexpensive computers built from general-purpose microprocessors. Unlike deterministic systems, a microprocessor-based device can do exactly what it is supposed to do and *many other things*. This makes verifying the functional correctness and fail-safe guarantees of microprocessor programs extremely difficult, and creates the possibility that some fraction of those *many other things* will include vulnerabilities that give attackers the opportunity to compromise the device and subvert its operation.

The transition from hardwired to general-purpose, from determinate to indeterminate, is at the root of computer system insecurity.

That insecurity can be addressed by driving hardware and software platforms towards more deterministic behavior. Doing so does not require replacing all microprocessor systems with their hardwired equivalents or expecting software makers to write perfect, bug-free code. Instead, it means favoring opportunities that increase a system's deterministic behavior.

Opportunities to leverage deterministic strategies include:

- **Maintain Critical Hardwired Components**: Deterministic systems used at critical points throughout a facility can reduce the potential for vulnerabilities that could impact system operation. Facilities can retain the benefits of deterministic systems by continuing to support their existing hardwired devices and by deploying verifiably deterministic hardware based on custom integrated circuits. The reliability, safety and security benefits of these deterministic components may provide operators with an additional justification for the continued deployment of hardwired and hardcoded components.
- **Read-Only Monitoring**: Microprocessor-based capabilities that provide networking and remote observation significantly enhance operational awareness throughout a facility, but their complexity creates the potential for exploitable vulnerabilities. In situations where monitoring systems are necessary, devices that operate in read-only mode can be deployed. A read-only monitoring device collects important information (temperatures, switch position, etc.) from an existing controller without modifying the deterministic behavior of the monitored controller. As a result, operators can maintain the functional assurances of critical systems while reducing the impact of vulnerabilities in the overlaid microprocessor systems.
- **Use Vulnerability-Eliminating Security Strategies**: As noted earlier, the security of microprocessor systems can be increased by removing unnecessary functionality, segmenting components, and integrating security protections. These strategies decrease vulnerabilities by making microprocessor devices and programs more deterministic - more likely to do exactly what they're supposed to do by eliminating some of their many other uses. These strategies can be applied to new and pre-existing microprocessor based systems as well as to read-only devices used on existing hardwired systems.

The various opportunities for implementing more deterministic behavior allow operators to select the strategies that best suit their needs. For example, facilities can retain non-networked, deterministic hardware. Facilities that are being upgraded can deploy deterministic hardware or read-only monitoring that will have limited impact on safety-critical components. Facilities that are already using microprocessors throughout their environment can be locked down using deterministic security tools and techniques. The result is that increasing a system's deterministic behavior improves operations by making critical components more reliable and increases security by limiting unexpected vulnerabilities.

Principle 3: Security Should Enhance Operations

Historically, the incentives for deploying security technologies have been completely misaligned with the operations team, who have been expected to spend increasingly large portions of their already limited budgets on security hardware and software that are only useful when their facility is under attack. Vulnerability-centric security takes the opposite approach: building and maintaining a strong cyber-defense is accomplished by placing the responsibility for security in the hands of the organization's existing operations team and increasing their effectiveness through strategies that both increase the facility's defense and enhance day-to-day operations.

The strategies used to implement vulnerability-centric security can enhance operations in the following ways:

- **Increase System Reliability**: Removing unnecessary system functionality, using read-only monitoring and continuing to support time-tested hardwired components reduces the potential for programming errors that can impact system operation. Segmenting system components through sandboxing and virtualization can prevent cascading failures by containing the consequences of an unexpected application crash. Integrating security functionality can alert developers and operators of malicious attacks and accidental software bugs enabling them to identify and prevent program failures during design, development, testing and in production.

- **Streamline System Management**: Sandboxing and virtualization technologies enable segmented applications to be configured, tested, packaged and deployed into production environments. Removing unused system functionality and deploying deterministic hardware and read-only devices reduces the need for ongoing support, testing, training and upgrades to those components. Security instrumentation can be integrated with existing application development, testing, verification and deployment processes.

- **Reduce the Need for Dedicated Security Technologies**: The tools and techniques used to implement vulnerability-centric security can be managed and maintained by a facility’s operations team. Deploying vulnerability-centric security technologies that both increase an organization's defenses and enhance the system's day-to-day operation allows facility personnel to concentrate on their top priority – ensuring the ongoing robustness and reliability of the systems they maintain.

There will never be enough security professionals to support attack-centric computer security because attack-centric security does not scale: throwing more people, time and money at ineffective security technologies will not make them effective.

The current push by academia, governments, and businesses to increase the number of security professionals will do little to benefit the nuclear security community. Conventional IT security specialists hired by nuclear system operators will arrive trained in the (incompatible) attack-centric security model, will not understand the constraints of the unique environment in which they are working, and will continue to be hired away by industries with bigger security budgets and higher salaries.

Placing the responsibility for computer security in the hands of the operations team addresses many of these concerns: the personnel are available, familiar with the unique system being defended, and have an established commitment to the success of the operation. Organizations with an existing safety team can receive a number of benefits from integrating computer security with that group. Combining safety and security allows the system-wide understanding of the safety team to be used in architecting a robust defense that utilizes existing processes for tracking safety requirements. Once those requirements are defined, their implementation can be integrated with existing safety procedures and exercises to ensure that security tools and technologies support the system's safety requirements.

Over time, increasing a facility's security and reliability should decrease the overall workload of personnel. As an added benefit, operations-enhancing security technology can be deployed using an organization's existing processes for introducing system maintenance, providing an established path for new security technologies to be selected, tested, placed into operation and maintained over time.

A Path Forward

The vulnerability-centric approach presents an opportunity for nuclear system operators to prevent successful cyber-attacks. Instead of constantly reacting to attacker innovations, operators increase their security by cutting down on their system's vulnerabilities. The mechanism by which vulnerabilities are reduced can be clearly articulated, verified and implemented using deterministic techniques that ensure system components only do what they are supposed to do - making the overall system more stable, robust and secure.

While attack-centric security degrades as new attacks are developed, the benefits of vulnerability-centric security accumulate as the number of system vulnerabilities decreases. Those benefits accumulate fastest on systems that change slowly, allowing nuclear facility operators to simultaneously drive their system's vulnerabilities towards zero while increasing its overall reliability.

In a world of complex computing environments, tight budgets and the potential for dangerous consequences, vulnerability-centric security enables nuclear facility operators to build and maintain a strong cyber-defense while enhancing the day-to-day operation of their systems.

Appendix: Vulnerability-Centric Security Technologies

Technologies to implement vulnerability-centric security strategies are available today and more are under active development. While there is no single technology that can eliminate every vulnerability on every system, the goal in developing a list of vulnerability-centric security technologies is to provide a starting point for operators to identify and build strategies that can be applied to their facilities.

Identifying opportunities to implement vulnerability-centric security does require an understanding of the available technologies in order to judge their applicability to a given facility. This knowledge may already be available to existing personnel in situations where currently-deployed technologies can be extended to provide vulnerability mitigation. Information on new technologies and approaches to identify and eliminate vulnerabilities may be obtained by personnel through ongoing skills development provided by nuclear industry and security organizations.

The following list briefly describes a selection of technologies that decrease vulnerabilities, increase deterministic behavior and enhance operations.

Hardware Virtualization

Virtualization enhances operations by providing new ways to monitor, maintain, migrate, test and deploy critical software while reducing the reliance on expensive, outdated hardware. This approach increases system security by reducing the unexpected behavior of physical computer systems and eliminating unused functionality (such as physical ports) and replacing potentially vulnerable legacy hardware and firmware with extensively tested virtual equivalents.

Hardware virtualization technology has become an established part of enterprise infrastructures and is the underlying technology behind the rise of cloud computing. Much of the work on virtualization technology has focused on virtualizing commodity hardware, such as those used to run the Windows operating system. New virtualization technology can be developed to virtualize more specialized hardware, such as those found in embedded devices.

Application Sandboxing

Sandboxing allows an application to run in a segmented software environment created specifically for that application. This can be performed by packaging the application inside its own self-contained environment (containerization) or using configurable operating system-level restrictions that use a security policy to describe the resources (disk, CPU, memory, network) the application is allowed to access. Sandbox isolation prevents unexpected application crashes (both intentional and unintentional) from impacting other applications on the computing device while providing system operators with enhanced auditing capabilities alerting them when unexpected behavior has been contained.

Rule-based application sandboxing systems have been supported by major operating systems, such as Linux, for the past fifteen years and has been adopted by newer systems such as the Android and iOS mobile operating systems. Container-based sandboxing is a relatively newer approach and commercial products exist that implement these capabilities on mainstream computer operating systems including Windows and Linux.

Software Scanning

Software scanning identifies bugs in a program by searching for errors in application code and monitoring programs in development and testing. Issues detected by software scanning can include exploitable security vulnerabilities as well as other programming bugs that could lead to unexpected system behavior such as program crashes.

Software scanning technology is almost as old as software itself, and in recent years there has been an increasing focus on refining these techniques to identify security issues. Vulnerability-centric scanning tools and services are available from numerous vendors, and, while the scanning process does not resolve software problems, the issues detected by the scanning process can be fed back to manufacturers for remediation or proactively resolved using security instrumentation techniques.

Security Instrumentation

Security instrumentation makes it possible to prevent and mitigate vulnerabilities in programs by inserting security functionality during development (e.g. capabilities programming) or after the code has been written (where the instrumentation is performed by the end user). The security-enhanced program will run exactly as its original form, however unexpected behavior, such as an attempted compromise or a program crash, can be identified while still allowing the program to continue operating.

These technologies are relatively new and have limited availability. Capabilities programming has been researched for the past decade and has recently been deployed in commercial applications and integrated into operating systems. The process of instrumenting existing programs to include security functionality is an area of ongoing research and development including the DARPA Cyber Grand Challenge.

Deterministic Hardware

The reliability, safety and security benefits of existing hardwired components can be recreated using custom-built integrated circuits. These integrated devices do not rely on complex operating systems and software. Instead they provide only the hardcoded functionality necessary to complete the device's task. These components can be crafted to segment critical functions from one another, designed to be easily reproducible, and can utilize numerous approaches to prove they behave as expected. Current design and manufacturing techniques make it possible for these components to be used as cost-effective replacements to internal components of legacy hardwired systems or in place of microprocessor-based devices running complex software.

Deterministic hardware such as FPGAs have been extensively used in the aerospace, automotive and medical industries. In recent years, these technologies have been the focus of increasing interest in the nuclear space, including the publication of IEC 62566 which offers guidance for the design and use of these components for safety systems in nuclear power plants.

Cryptography

Cryptographic protections can provide mathematical guarantees that operators and system applications are only capable of performing authorized activities. This is made possible through protections at multiple points in a facility including cryptographic authentication of users, encrypting network traffic and integrity checking of both programs and network communications.

Many of the protections made possible by cryptography are already available in the form of public algorithms, protocol specifications and functionality built into mainstream operating systems. The opportunities for cryptographic protections may be limited in some environments by the processing power and network bandwidth necessary to implement their operation.