Indiana University School of Informatics and Computing

HATS Research Department

SDN: Battlefields Case Study Writeup

Battlefield Use Case

The Armed Forces has widely varying network contexts. There are the established networks, from Pentagon to Pacific, that are either classified or unclassified. Classified networks ideally are implemented with an air gap. Unclassified networks are in a state of cyberwar. It is the state of assault by nation-states and actors with equivalent resources that distinguish this use case. Economics of attack and defense are arguably inapplicable when the adversary has effectively unlimited funds and is not seeking monetization.

A second, similar category of networks are ones that are established, but mobile. These networks include the ones found on naval ships. Unlike the first category of networks, these have to operate under very strict limitations. Equipment failures cannot be fixed by simple replacements if a vessel is thousands of miles from the nearest friendly port. Therefore, equipment must undergo rigorous certification procedures, making tasks as simple as firmware upgrades long, arduous procedures. Additionally, the rigid requirements of the network make enforcing network compliance a difficult task when housing personnel that bring their own devices.

The final category of networks of interest are those that must be immediately deployed, often in domains with little preexisting infrastructure. The preexisting infrastructure may be putatively under the control of allies; however, even in this case the insider threat is so extreme as to make these network components effectively untrustworthy (e.g. vehicles in the front lines of combat). In this case operators themselves are untrustworthy without considering the more fundamental question of SDN as allowing trusted operations on untrusted hardware.

Operators and Stakeholders

At the most fundamental level, the operators and stakehodlers in the battlefield or disaster preparedness case are the people in the boots on the ground. Too formal a set of requirements for the devices software as a service will result in subversion. The capacity to isolate the networks that are created by personnel bringing their own devices combines these. For example, requiring that no personnel bring any gaming devices to extended deployments may appear a reasonable policy, particularly to senior officers whose childhood included more Parcheesi than Princess Peach. However, such constraints are likely to be subverted in practice. Individuals in high-stress and high-risk situations are more likely to subvert policy for their own requirements for communication and stress release. Currently, the vast majority of security policy violations are in the theater. By creating the possibility of true isolation between bring-your-own-device networks and the operation networks, SDN offers the ability to set appropriate multi-level requirements. Recognizing individuals in the field with their own devices as legitimate stakeholders can be integrated into a resilient SDN.

A second set of stakeholders are allies who may include less trusted insiders who are working with military personnel. The tragic increase of blue on green violence in 2012 is testament to the limitations of political alliances to ensure allegiances of individuals. Because of the complex interaction of political and military, proximity authentication and requirements are quite distinct from the commercial domain.

At a higher level, stakeholders include the operators of classified and unclassified networks. For military networks this includes identity providers and trusted certificate providers. Included here are those who test, maintain, and upgrade the networks. The short product lifecycle characteristic to information technology exacerbates the conflict of interest between network operator and those responsible for

assurance. As new products and methods of communication become available to individuals in the field, those responsible for authentication find the laboratory assumptions no longer hold. A firewall that is secure today may see the creation of a tunnel by a new consumer innovation brought by a member of the National Guard; which then allows an attacker through the network into the less secured interior. An action as simple as upgrading the browser may be necessary for security or may instead introduce a range of vulnerabilities.

Testing and upgrade components are unique and critical to the defense space. Formal auditing expense and difficulty is a critical barrier to adoption and upgrading of military systems. SDN offers the ability, in the production of few core hardware components, to implement a wide range of network functionality while keeping the complexity of the firmware on network hardware relatively simple and static. For example, a new routing protocol can be implemented in the controller and applied to the entire network without any firmware changes to the network hardware.

Battlefield networks have a distinction that may allow for more effective use of SDN: a hierarchical network of distributed authentication tokens or 'cat cards'.

Technical Operations

The three components of threats above match to a higher-level conceptualization of SDN.

The closing air gap between classified and unclassified networks is a case of secure secure internetworking. The essential functional requirements are isolation and ideally even invisibility.

Compartmentalization is a requirement for multiple SDN applications, such as cyberphysical systems. In the Next Generation Battlefield there is a requirement for dynamic compartmentalization. As components are added or become unreachable the system must retain the original security policy. The system not only will maintain its integrity but also be able to introduce new elements quickly. In a chaotic environment being unable to use the network may be life threatening in the battlefield. Users unable to use the network may also use insecure channels if the system is unreliable or inflexible. The Next Generation Battlefield requires Battlefield and other defense networks may need to greatly increase capacity and number of elements. For example high volumes of visual data may need to be transmitted and analyzed to deal with a new physical threat.

Currently, DoD networks require extensive change management procedures and require significant analysis of any change made to a network to determine the impact on security. SDN technologies may allow for the rapid reconfiguration of the network to add additional circuits and network hardware. The logically centralized controller topology allows new components to be added without having to verify the entire system. Conformance can be broken down into multiple separate tasks of ensuring the security policy is being maintained by the software; ensuring secure, reliable connectivity; and verifying the network device properly enacts the rules specified by the software. The core value of SDN, that is networking logic that is hardware agnostic, inherently aligns with the testing and upgrading requirements for configuration management. Hardware upgrades would no longer require extensive testing of various network protocol implementations on the hardware; and, conversely, network software changes can be made without having to upgrade and test the hardware. SDN specifications provide a clearly defined common denominator that hardware manufactures and software engineers can target to guarantee interoperability between the two.

The air gap between classified and non-classified networks is closing. Deployed tactical systems seek isolation and invisibility from other networks, as opposed to more classic requirements for assurance. Open-Flow offers the exact specification of what can be connected. Imagine connecting an external subsystem that only needs to talk to one or two devices or systems. In a SDN network it would be possible to leverage the existing ethernet infrastructure to allow the new external subsystem to address

only those that are desired, and indeed to find only those for which connections are desired. The closure of the air gap is a challenge of **internetworking resilience.**

Physical reconfiguration is a unique challenge on the battlefield because it occurs at high stress moments during physical attack. Orchestration and automatic reconfiguration provide ways to mitigate the issues of network reconfiguration under battlefield conditions. SDN controllers and other orchestration systems could react to the changing conditions and automatically reconfigure the network and and other resources. SDN networks can resist to degradation such as radio interference of the communication channel by using redundant transmission of the message of different frequencies or type of transmission technology.

Weaponry and armor will be networked, as exemplified by the goals of the Joint Tactical Radio System. The ideal of every soldier being a data command point with the ability to send and receive data-rich images and to provide different ways to communicate. The increased use of large data flows from many different sources and receivers makes the networking more difficult. Not only does the network have to handle increasingly large data flows the direction of the information has changed. Information gathering and retrieval can be done at any location giving each soldier a greater awareness of the battlefield conditions. However reliability, security and performance of the network transmitting this information needs to be assured. Multipath transmissions may allow greater bandwidth utilizing all possible paths to transmit high priority information. Critical transmissions can receive guaranteed bandwidth or utilize quality of service parameters configured in a SDN protocol.

Vulnerabilities

While it is the case that network service providers and data centers require isolation, these are much less likely to face advance, persistent threats of the nation-state level. It is certainly the case that physical attacks are a unique concern.

The military network is characterized by hardware tokens that identify individuals and devices. The unique vulnerability is that these can be captured and not identified as being held by hostiles. Captures of individuals, devices, and tokens are serious issues. In the battlefield, possession of devices can change suddenly and not be detected for hours.

Information sharing requirements in the military do not map directly to industry requirements. In the case of isolation it may be acceptable for a line employee to be isolated, and to wait for technical assistance. However, such delays are not tolerable in the battlefield or emergency environment. Conversely, overcommitting to resources is a standard approach to deployed network configuration. Thus the capacity to isolate quickly upon risk of subversion may be more acceptable in a military domain than in an industrial application. Perversely, more than any other domain, respect for the restraints on attention span are most critical in a battlefield.

- The Black Box Full characterization and qualification of a component (e.g. NIC, switch, router, etc) is made difficult by elements of the component that cannot be subject to full inspection and classification. These potentially unknowable elements regularly include firmware and programmable logic devices. Mitigations to the black box problem often include high-coverage testing and guard elements which increase system cost and development time. These mitigations increase cost, and must be repeated for every new device connected to the network. As different generations of hardware connect to the network, it becomes more challenging to examine every possible interaction.
- Configuration management Even very minor changes to a systems hardware or software configuration can bring about very significant changes in behavior. For this reason, configuration management in critical real-time systems is a high priority. Commercial-of-the-shelf (COTS) products often have no requirement or incentive to maintain configuration management. In fact,

the pressures of the commercial domain (cost priorities and lean operating principles) often creates an environment that is not conducive to constraints on configuration.

- Coordinated (and restricted) interfaces Large systems often categorized as systems of systems often have independently developed subsystems that rely on highly-coordinated interfaces. While many commercial standards (IEEE 802.3 is just one example) meet the performance requirements, use of such powerful interfaces presents a large threat surface and an enormous testing challenge. Accordingly, such broad interfaces must be profiled to assess the necessary subset of features that are required and subject to validation. Similarly, there is interest in managing interfaces such that subsystems can- not be easily spoofed. There has been interesting work in this area that includes domain specific languages (DSLs) (see Meredith Patterson 28C3 talk). This is exacerbated but the challenge that military authentication does not happen at the network level. It happens with certificates on the machine, using certificates across the network, and in informal (often policy-violating) interactions in the field.

Organization Requirements

The reality of military configuration is that preparation may have high levels resources, capacity for testing, and well-controlled authentication before configuration. However, many of these will be highly compartmentalized in order to prevent an internal adversary or inadvertent leakage to provide information on scale or participants of an action. Once an action has begun, and at any moment after initiation, moment of reconfiguration are extremely likely to be associated with cognitive overload and data uncertainty.

- The Black Box SDN, or more specifically OpenFlow, implementation could allow a standardized method of interfacing with the hardware component, eliminating unique programming interfaces for different devices. Use of SDN could allow for standardized test cases which could be used across multiple products with minimal change driving commonality during evaluation and qualification.
- Configuration management By constraining the actions a priori the behaviors of a device can be constrained, and should a device exhibit behaviors beyond its constraints then it can be disabled or removed. This allows an organization to place integrity or confidentiality above survivability; and to develop a flexible policy for these trade-offs in different situations.
- Coordinated (and restricted) interfaces The hardware devices and pre-configuration can provide necessary isolation in daily operations. However, it is famously true that no operational plan survives actual engagement. Adding real time level of authentication can enable the network to provide more fluid permissions. Combining the hardware with social engagement in defined operational situations can enable robust responses to changes in operation. For example expanding x590 to include some human-readable but network-authenticated challenge-respond to enable the level of human authentication that is necessary can limit misuse of automated recognition of captured devices, but create a level of vulnerability to social engineering. Examination of trust mechanisms beyond the isolated technical certificate is necessary to address the integration of cultures (e.g., different regional first responders or allied forces) and organizations.