Case Studies

1. CASE STUDY 1: SSL VPN SOLUTION PLANNING AND IMPLEMENTATION

This case study presents SSL VPN solution planning and implementation. The case study begins by describing a real-world security requirement scenario: protecting network communications between remote users and a main office. The case study then discusses possible solutions for the security requirement and explains why an SSL VPN architecture was selected over the alternatives. The next part of the case study discusses the design of the solution and also provides some details of the implementation of the solution prototype, including examples of configuring the solution using commonly available equipment and software.

The case study is not meant to endorse the use of particular products, nor are any products being recommended over other products. A fictional combination of several common products was chosen so that the case study would demonstrate a variety of solutions. Organizations and individuals should not replicate and deploy the sample entries. They are intended to illustrate the decisions and actions involved in configuring the solutions, not to be deployed as-is into systems.

The organization already offers remote access services in the form of a host-to-gateway IPsec solution. This works successfully but has required significant IT labor resources to install and support the client software on user hosts. The current solution also does not provide remote access for hosts based in public locations such as hotels and kiosks. The organization is therefore looking to implement a complementary remote access architecture.

2. CHALLENGES

The organization specifies its organizational requirements for remote access:

- All users should have access to all internal network resources, especially email and calendar services. This open policy is necessary because of the broad range of IT resources required by users to conduct their research. Users may also be required to authenticate themselves to specific resources such as file shares and databases.
- Users should only have access to a limited set of internal services such as email and calendaring if they are using public hosts (hosts located in environments such as hotels and Internet cafes).
- A small population of users outside of the organization and human resources (HR) staff from the parent organization, should have access to a limited set of internal HR applications.

3. SOLUTION

Network Layer Solution: IPsec VPN

As previously mentioned, the organization has already established IPsec-based network layer VPN services for remote users. Many users are satisfied with this solution, but it can be cumbersome for IT staff to support because each host requires client software to be installed and supported. Moreover, hosts without the preinstalled client software cannot access internal resources.

Transport Layer Solution: SSL VPN

The organization could provide an SSL VPN between the remote users and the office over the Internet. Network extension is the most flexible option because it provides broad access for users into an internal network.

Application Layer Solution: Application Modification

The organization could modify every application required for remote access. Applications such as SSH are already supported for remote access. Due to the broad range of relevant applications, it is not considered feasible to modify all of them.

The organization decides to develop an SSL VPN solution. This solution will complement and not replace the existing IPsec VPN services. It is assumed that some users will stay with the IPsec solution, but others will migrate to SSL VPN over time. The organization purchases a commercial appliance with a support contract to ensure the existence of vendor support.

Designing the Solution

The organization goes through a process to design the SSL VPN solution. It first designs an access control policy to determine who can access internal resources and under what conditions. The next step is to create an endpoint security policy that enforces access control, usually with host integrity checks. Creating an authentication infrastructure, designing the architecture and deciding on encryption, are the last steps.

Access Control Policy

The organization goes through the four major steps to designing an access control policy:

1. **List the resources that will be accessed through the SSL VPN.** Users should have access to all internal network resources, so these resources can all be grouped together. If a specific resource such as a file share or database requires additional authentication, then this takes place when a user accesses the resource. The only exception to this policy of grouping all resources is a set of HR applications that only a small set of external users is authorized to access. Note that these users may not access the other internal resources that other users can access.
2. **List the groups or users.** Most users are in one main group that has network connectivity to all internal resources. A smaller group is composed of external users that have access to the set of HR applications mentioned in the previous step.
3. **List the conditions under which the resources should be accessible by the groups.** There are several conditions for accessing resources:
   - Users must use hosts managed by the organization to gain access to internal resources. These organization-managed hosts all have a system registry key installed that can be checked to verify their identity.
   - Users who login from systems in a public location such as a kiosk or Internet café or use their personal computers can only access a limited set of Web-based applications such as email, calendaring, and employee phone directory.
   - The small group of external users that access the HR applications must also use organization-managed hosts to gain access to these applications.
   - All hosts, public or otherwise, must be running the latest version of Windows with critical security updates installed and an antivirus package with an up-to-date virus signature database. They must also have a firewall program installed and running. Any host not meeting these requirements is not permitted to login.
4. **List how the VPN should be used to access the resources.** Resources are accessible in different ways:
   - The organization's internal resources are accessible by network extension because a broad number of them are hosted on multiple servers. Also, some Web-based applications do not function properly when proxying is used, so network extension must be used.
   - When users login from public hosts that are not organization-managed, they can access a set of Web-based applications via proxy.
   - The set of HR applications are accessible by network extension because some require many interlocking programs and cannot be accessed by other means.

Endpoint Security Policy

The organization designs an endpoint security policy to enforce access control. The policy is mainly driven by a prelogin sequence executed by the SSL VPN appliance before a user logs in. This sequence runs host integrity checks that require the host to download and run active content controls. These controls or applets ensure that the host complies with the organization's endpoint security policy.

The endpoint security policy is based on the access control policy and elaborates further: An organization-managed host is identified by a registry key indicating that the host is managed by the organization. The host integrity check only needs to find this key to verify the host's identity. Organization-managed hosts use network extension to gain full access to the internal network. A packet filter is configured on the SSL VPN to prevent these hosts from accessing the restricted set of HR applications. If a user is permitted to use the restricted set of HR applications, a packet filter is configured on the SSL VPN to prevent the user from accessing any resource outside the HR applications. Users are permitted to keep all cookies, Web browser cache entries, and downloaded files and attachments.

A host that is not organization-managed or is personally owned can only access Web applications via proxy. The SSL VPN session is established in a virtual storage space and all data stored or downloaded during the session is erased after logout.

All hosts must run one or more specific versions of Windows, with each specific version using the most current set of updates. Critical security updates are also required to be installed. The host must run an antivirus software program certified by the organization that is active and uses a virus signature database that has been updated in the past month. The host must also run a firewall program.

Authentication Scheme

The organization has an existing RADIUS authentication infrastructure for multiple resources such as databases and email servers. The SSL VPN appliances use the same RADIUS servers to authenticate users as they login to the SSL VPN portal. The groups that are defined by the access control policy are configured in RADIUS. So most users belong to one large RADIUS group, and the external users granted access to the HR applications are put into another smaller RADIUS group.

The SSL VPN appliances determine this group information from RADIUS so they can dynamically map users into the correct group. For example, a user who is a member of the HR Users' RADIUS group is only given access to the HR applications.

Users authenticate themselves via two-factor authentication. Each user must type in a password and use a physical token to enter a one-time password generated by the token. For server authentication, the organization purchases an SSL server certificate from a CA whose root certificate is already installed in most common browsers and installs the SSL server certificate on the SSL VPN appliance.

Architecture Design

The organization designs an architecture incorporating the SSL VPN appliances within its existing network infrastructure. It performs configuration of the appliances and devises a management policy.

Selection of Hardware Configuration

The organization chooses an appliance solution developed by a commercial vendor. Hardware appliances are the most common type of SSL VPN hardware on the market today, and they possess the advantages of being preconfigured and already hardened by the vendor. Furthermore, support is more straightforward because the device configuration is standardized.

Device Placement and Firewall Configuration

The organization adopts an internal SSL VPN approach for device placement. Access to TCP port 443 on the SSL VPN for all external addresses is added to the corporate firewall; no other access rules are added to the firewall.

Routing Policy

The organization prohibits split tunneling, so the remote access host sends all traffic destined for internal subnets and the rest of the Internet through the VPN tunnel. Traffic destined for machines outside the organization's perimeter is blocked by the SSL VPN. In this case, attempts to go off the corporate network directly from the user's system are blocked. Some SSL VPNs include *hairpin proxies* that allow VPN users to leave the network, but only by traversing the SSL VPN gateway, which has been set up as a normal outgoing firewall.

The organization has a main headquarters location and several branch offices, but it only deploys SSL VPN appliances at headquarters. All of the organization's internal IT resources are available at headquarters.

High Availability

The organization is pursuing a high availability strategy. The VPN appliance supports high availability with an active/passive architecture. Configuration settings are mirrored across both devices, so any configuration change made to the active device is automatically copied to the passive device's configuration. VPN session information is also mirrored; users do not have to reauthenticate after a device failure, but existing TCP connections are broken and do have to be reestablished.

Management

The management policy for the VPN appliances is consistent with the organization's security policy. Administrative access is only supported on the appliance's internal interface and is limited to a small set of IP addresses. Accounts with limited administrative access are created and assigned to different groups, such as one account that can review system logs and another account that can update the host integrity checks to search for recent security updates.

Configuration settings are backed up each week to a central server. The organization also uses a set of appliances for testing and staging. They are configured identically to the live units, and any updates or patches are applied on them first.

The appliances are monitored by the organization's network management system. The network management system periodically pings the appliances' IP addresses and polls the appliances' SNMP management information base (MIB). It compares data from the MIB with known operational values to search for any potential operational issues.

Client Software Selection

The prelogin sequence requires a remote access host to download and execute active content so the host integrity checks can be performed. The desktop management policies for the organization-managed hosts are configured to permit specific active content controls to run locally.

Portal Design

The organization uses the portal provided by the VPN appliance vendor. It provides some customization such as altering the banner graphics to be consistent with the organization's logo and colors. It also only displays options that the user is authorized to access. For example, if a user is in the group that is only allowed to view the HR Web sites, only those sites are listed on the user's portal page.

Encryption Scheme

The organization requires FIPS 140-2 compliance for its SSL VPN solution. As a result, the organization verifies the level of FIPS compliance of the system before purchasing it. The organization configures the SSL VPN to only permit logins from client browsers that use SSL cipher suites with FIPS-approved cryptography. The appliance is also configured to require browsers to support TLS 1.0 or higher for SSL connections.

Implementing a Prototype

After the organization designs the SSL VPN solution, it implements and tests a prototype of the design. The prototype is initially configured and tested in a laboratory network and is moved later to a production network so access to actual internal resources can be tested. The laboratory network replicates the addresses of the corporate network, and thus needs to be completely unconnected to the corporate network. The test network includes a firewall with the same configuration as the corporate firewall, and example servers that have the same capabilities and the same addresses as the servers that will be accessed through the SSL VPN.

The organization develops a test plan to evaluate functionality and connectivity. The plan includes tests for connectivity, authentication, access control, endpoint security, and client interoperability. Users of multiple operating systems (Windows, Linux, Macintosh), device types (laptops, PDAs, smart phones) and Web browsers (Internet Explorer, Firefox, Mozilla, Safari) must be able to access internal resources from outside the network. If users are using organization-managed hosts, then they should be able to do everything they could do if they were located in their offices. Multiple scenarios such as a user logging in from a public host or a host that has an out of date virus database must be tested. The testers also validate that people with different types of RADIUS credentials only get the expected type of access when they log in during the test.

Example Configuration Steps

Different SSL VPNs have different administrative interfaces. Many allow control through Web browsers, while some use custom programs, and still others use old-style command line interfaces (CLI). In this part, a fictitious SSL VPN that has a browser interface is described along with examples of steps that might be taken to implement the rules from the scenario. The interface has four major sections:

1. System
2. Users
3. Access
4. Policies.

To begin, the administrator needs to configure the addresses of the Ethernet interface on the SSL VPN. The administrator goes to the *Ethernet* choice in the System menu and sets the address assigned to the SSL VPN on the inside of the corporate network. Because this system is configured inside the existing network, no routing needs to be defined; had this SSL VPN been located outside the firewall or on the DMZ, the administrator would need to specify routing information.

Using the *Add User Group* choice of the Users menu, the administrator creates a group called "NormalUsers". In this dialog box, the administrator specifies which authentication mechanisms are used (a password and a physical token) and specifies how the authentication is validated (using the existing RADIUS server). The administrator specifies that participation in the NormalUsers group for the VPN is given to people whom the RADIUS server labels as "User". They use the Add User Group choice to add a second group, "HROnlyUsers", but participation in that group is the people the RADIUS server labels as "HR Users".

The Access menu allows the administrator to define those resources to which the members of each user group have access. Using the *Add Access Group* command, the administrator creates an access group called "NormalFullAccess" that links "NormalUsers" to all network services, using a network extension program from the SSL VPN. The network extension's packet filter is set up to block TCP ports 80 and 443 of the addresses of the Web servers that are controlled by the HR department. The administrator also selects *only display available resources* for this access group.

Next, for users accessing the SSL VPN from equipment that is not owned by the organization, the administrator uses the *Add Access Group* command to create an access group called "NormalPartialAccess" that links "NormalUsers" only to TCP port 80 of the addresses for the three Web servers that have the corporate calendar, the Web mail system, and the employee phone directory,

using a reverse Web proxy, and selects only *display available resources*. Last, the administrator creates the "HRAccess" group that links "HROnlyUsers", using a network extension program from the SSL VPN to allow access to only TCP ports 80 and 443 of the addresses of the Web servers that are controlled by the HR department, and selects *only display available resources*.

The three access lists each have policies associated with them, so the administrator uses the *Policy List* command in the *Policies* menu to create a list of policies. The dialog box starts with an empty list, and the administrator clicks the *Add* button to create the first policy. In that dialog box, the administrator specifies that everyone in the NormalFullAccess group must use the following policies:

- The remote host is managed by the organization.
- The latest version of one or more specific versions of Windows is being used.
- The most current set of patches and security updates has been applied to the operating system.
- An approved antivirus program is running.
- An approved firewall program with an approved configuration is running.
- Split tunneling is not permitted.
- The protocol used must be TLS 1.0 or later.

The cryptographic protocol being used must be one that complies with FIPS 140-2. After creating this policy, the administrator creates similar policies for everyone in the NormalPartialAccess and HRAccess groups.

The last steps are to configure the management of the SSL VPN itself. In the *Administrators* command in the System menu, the administrator changes the default password that came with the system and sets the range of IP addresses that can be used to administer the system. In the same dialog box, the administrator also creates additional administrative accounts with limited rights, such as for viewing particular logs. Under the *Backup* command in the System menu, the administrator sets up automatic weekly backups to be sent to an FTP server on the internal network. The *SNMP* command in the System menu is used to allow monitoring of the device.

The *Replication* command in the System menu allows configuration of the high availability feature described earlier. The administrator enters the address of the other server in the high availability group and specifies that this server is the "master" of the group.

Deploying and Managing the Solution

The organization employs a pilot program to deploy the solution. It solicits volunteers who can contribute their user experience and help to troubleshoot any problems with connectivity or interoperability. The SSL VPN development staff also produces documentation to help in establishing VPN connectivity. The documentation assists users in enabling the host integrity checks to be executed on their hosts, and it addresses frequently asked questions.

Conclusion

This case study covered planning and implementing an SSL VPN system for an organization. The steps described in this case study follow the recommendations and guidelines given for choosing and setting up an SSL VPN. It should be emphasized that the scenario described in this case study is for a fictitious organization and that the steps taken by a real organization would likely be different from those given here.

The portrayed organization first identified its needs based on its current operations and its stated future goals for secure remote access. In designing the proposed solution, the organization followed the typical steps of creating both an access control and an endpoint security policy: laying out its methods for authentication of users; designing an overall architecture for the expected remote access solution; selecting the hardware needed to meet its goals; specifying where in its current network the hardware will go; determining whether or not it needs a high availability solution; creating a management policy for the system and users; selecting the client software; designing the portal that the users will see when they connect to the system; and, developing an encryption policy.

After this design was completed, the organization implemented a prototype of the system before deploying it fully. The test plan for this prototype involved creating a sample configuration for the network access, the list of users for the system, definitions of the types of access that will be given to the users, and a specific policy plan linking the users to the types of access as well as other policy restrictions on the users.

4. CASE STUDY 2: CYBER ATTACKS ON CRITICAL INFRASTRUCTURES—A RISK TO THE NATION

There has been a great deal of research related to cyber attacks and vulnerabilities and critical infrastructure, but there is an incomplete understanding of the cascading effects a cyber-caused disruption could have on other critical national infrastructures and the ability of the affected infrastructures to deliver services. Sandia National Laboratories (Sandia) has developed methodologies that translate a cyber-based disruption to a physical disruption of infrastructure and economic methodologies that can provide an understanding of the national-level risk from cyber attacks on critical infrastructure. This case study

discusses these methodologies, and addresses these methods' gaps for correlating cyber attacks with physical and economic consequences in the nation's critical infrastructures. This case study further explains Sandia's roadmap to fill the methodological gaps, beginning with the electric power grid and then extending to other infrastructures.

5. CHALLENGES

This part of the case study describes a cyber-attack-consequence assessment process developed to coordinate Sandia's capabilities in assessing the effects of a cyber attack and in assessing the infrastructure impacts and economic consequences of those attacks.

Step 1 of this process identifies a cyber attack, and Step 2 identifies a system vulnerability that will allow a cyber attack to be successful. These two steps may occur simultaneously because a cyber attack is likely to attempt to exploit a system vulnerability to ensure success.

Step 3 of this process is the assessment of the effects of a successful cyber attack on a critical infrastructure control system. This step answers the question "How does the attack affect the control system and the components that are connected to the system?" Simulators that model control systems can be used to assess how the control system will react to the attack. This step can be informed by general heuristics, or rules-of-thumb, about the structure of the control systems to help inform the assessment.

During Step 4 of the process, the impact of the control system effects to the critical infrastructure being attacked (and possibly other, related infrastructure) is assessed. Infrastructure models are used to determine how the control system effects might spill over to other parts of the infrastructure that are not controlled by the attacked system. The result of this step is an infrastructure-impact scenario, which is a specific scenario of how the infrastructure is affected by the cyber attack. The scenario should specify the particular components of the infrastructure that are affected, as well as the details (time, severity, etc.) of the impacts.

Finally, during Step 5 of the process, the economic consequences of the infrastructure disruptions are found using the infrastructure-impact scenario. If the infrastructure-impact scenario constructed in Step 4 finds that the cyber attack may create disruptions in infrastructure, there will likely be economic ramifications to the loss. Economic models are available that can be used to assess the economic consequences of infrastructure disruptions caused by cyber attacks.

Process Walk-Through with Electric Power

This part of the case study explains Sandia's walk-through of the cyber-attack-consequence assessment process, using electric power as an example. Sandia's existing capabilities make this process relatively straightforward to accomplish for electric power.

Sandia has developed extensive capabilities for simulating electric power control systems through its participation in the National SCADA Test Bed (NSTB). NSTB is a multinational laboratory facility created by the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE). A mission of NSTB is "identify[ing] and correct[ing] critical security flaws in SCADA control systems and equipment." Facilities are concentrated at the Center for Control System Security at Sandia and the Critical Infrastructure Test Range at Idaho National Laboratory.

The NSTB was created "to assist the energy sector and equipment vendors in improving the security of control systems hardware and software" and "has closely aligned its activities with industry-defined priorities. This part of the case study will also discuss how the capabilities that the NSTB has developed to model the effects of cyber attacks on physical assets, can be extended to explore how physical disruptions may cascade across infrastructures and assess the economic consequences of those disruptions.

Cyber-Attack and System-Vulnerability Steps

In the first two steps of the process, a cyber attack is identified along with the vulnerabilities in the control system that it may exploit. Because the Sandia report is most concerned with creating a roadmap for the final three steps of the process, it is assumed that these steps have been completed, and the results are available to inform the remaining steps of the process.

An example of results that may come from this step for an attack on electric power control systems is given in a scenario. In the scenario, multiple malevolent front-end processors (FEPs) have been compromised at the manufacturer or through software updates. An FEP is a computer that provides a bridge between client computers of human operators and power system hardware clients such as remote terminal units (RTUs). The FEP passes commands from the users to the hardware and provides the user with data from the power system hardware. The rogue FEPs are programmed to send breaker trip commands to generators, in order to induce widespread under-frequency load shedding during periods where power reserves are low (Stage 2 alerts), thus causing blackouts.

System Effect

Step 3 of the process assesses the effects of the cyber attack on the control systems being attacked. This step

can be informed by heuristics about infrastructure interdependencies that may facilitate the cyber attack. For example, if a utility's control systems were networked to computers that had Internet access, it would be possible that a cyber attack against that utility might affect the control systems, even if the attack was not directly aimed at those systems. Protected Critical Infrastructure Information (PCII) information collected from Department of Homeland Security (DHS) site-assist visits is a source of these data. These data are stored at Argonne National Laboratories.

The effects of cyber attacks against control systems can currently be assessed for electric power using the Virtual Control Systems Environment (VCSE), developed by Sandia as part of the NSTB program. The focus of VCSE modeling has been electric power control systems.

Infrastructure Impact

Cyber attacks can impact not only the entity that they attack, but other entities within the same infrastructure. These impacts can cascade into other infrastructures. The cumulative effect of these infrastructure disruptions will likely have an impact on the economy.

Disruptions in electric power are especially susceptible to spillovers. There are a limited number of alternating-current (AC) power grids in the contiguous United States. All components of each grid must operate in concert with one another, at the same frequency. Deviations in frequency or voltage may cause circuit breakers to open to protect equipment, which may further exacerbate the deviations, thus leading to a cascade of failures.

The NSTB currently has capabilities for assessing the impacts of cyber attacks on the electric power grid. The VCSE has the ability to interface with external software that simulates infrastructure systems. For example, in the cyber attack scenario developed in the *National SCADA Test Bed Threat Development Team, Threat case scenario*, a steady-state, loadshedding model is used to simulate the effects on a power grid. The VCSE also has the capability to interface with other software that can simulate infrastructures beyond power.

In this walk-through, the result of the system-effect step, coupled with the results from the VCSE, can be used to construct an infrastructure impact scenario for the impacts of a cyber attack on electric power. This scenario can be augmented to include the impact on other infrastructure through the use of the Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool (FAIT).

Economic Consequences

A cyber attack on a control system may have effects beyond those of the attacked infrastructure identified in the infrastructure-impact step of the process. Infrastructures are interdependent, which means that a failure in one component may spill over to other components of the same infrastructure as well as associated infrastructures and industries. This interdependence is clear in the electrical power industry because almost all industries require electrical power in some manner. Disruptions of infrastructure may also spill over to economies. Economic activity depends on the infrastructure. A sustained loss of electric power, for example, may cause economic activity to nearly stop.

The consequences of infrastructure disruptions are complicated and difficult or impossible to measure in many cases and may vary greatly in their consequences. An outage at a single generator during a period with adequate reserve capacity is unlikely to disrupt service. Spot prices might be affected by the outage, but there will likely be little change to overall economic activity. The consequences of an outage that results in unserved load are more difficult to measure. For a short load-shedding event, the economic consequences will likely be light because many short-term economic losses are recoverable. For example, consumer purchases can be delayed to another day or time, and interrupted manufacturers can draw on inventories that can be replenished over time. Many of the losses that do occur may be difficult to quantify. For example, short losses of power chemical plants sometimes cause the release of chemicals and have the potential to cause accidents.

In the case of electric power, smaller outages are likely to affect a small area and last a short time. Consequences of the power outage are likely to be relatively small and affect a small number of parties. Identification of the consequences will, therefore, be difficult. On the other hand, a large blackout that lasts a long time will have larger consequences that affect nearly all infrastructures and individuals. Consequences identification will be much easier because of the importance and ubiquity of electric power.

In the NSTB workshop, some informal methods of assessing the economic consequences of cyber attacks to electric power systems were developed using the scenario in the *NationalSCADA Test Bed Threat Development Team, Threat case scenario*. The purpose of the exercise was to estimate the consequences of a cyber attack on a single utility company, rather than estimating the economic effects to the entire economy. A low-fidelity proxy for the cost of lawsuits due to a day-long blackout to the utility's entire service territory was created by calculating all of the direct and indirect economic impacts in the service territory. In reality, the effects of a cyber attack are likely to be more complex in terms of the coverage and duration of the blackout. Furthermore, the economic impact of the blackout is unlikely to be a complete loss of

all economic activity, especially for short-duration blackouts. However, economic losses may propagate beyond the immediate service area.

Gaps in Capabilities

There are several limitations to the capabilities described in the walk-through of the cyber attack-consequence assessment process for electric power. These gaps can be closed using capabilities that currently exist or are under development at Sandia. Closing these gaps will often add complications to the process because the gap-closing tools are more complex than those used in the walk-through. Researchers will need to decide whether the improvements to the results of the process (the infrastructure impact scenario and the measurement of the economic consequences) are worth the costs of the increased complexity.

Use of Unrealistic Power Grids

The Institute of Electrical and Electronics Engineers Reliability Test System-96 (IEEE RTS-96) power grid model, which is currently used by the VCSE steady-state simulator, is not a representation of a true power grid. The IEEE RTS-96 specification is just one possible specification, and it is chosen so that it simulates most features that exist throughout power grids. However, this specification is not a realistic representation of any actual grid. The IEEE RTS-96 specification contains generators with a total generating capacity of 10,215 megawatts (MW), which is much smaller than actual power grids. For example, the load that was lost in the Northeast Blackout of 2003 was 22,984 MW in the state of New York, alone. As with the power grid test bed, there are no associated infrastructures or economies; therefore, it is difficult to create infrastructure-impact scenarios that can be used to map power system impacts to infrastructure and economic consequences. Rules-of-thumb for the costs of outages to customers can be developed, but these rules are not specific to any particular scenario and include only direct economic impacts.

Other electric power models, in use or being developed by the NSTB at Sandia, use IEEE RTS-96 or specifications that are even more limited than IEEE RTS-96. While these models are useful for conducting experiments to see how cyber attacks affect electric power control systems, it is difficult to construct infrastructure-impact scenarios. Thus the models in use create a barrier to accurate consequence assessments.

The use of true-to-life power grid models would allow improved infrastructure-impact scenarios that would rely less on researchers' intuition. The steady-state model applied to IEEE RTS-96 produces estimates of hypothetical loads loss. A researcher has to decide how that maps to real world loads. If the steady-state model were applied to a real power grid, the output of the infrastructure simulation would show which loads were really lost. These areas could be mapped to counties and inputted into Regional Economic Accounting (tool (REAcct)) with a minimal number of additional assumptions.

Models of Electric Power Grids are Limited

The VCSE steady-state electric power model used in the earlier walk-through does not model the dynamic behavior of the power system, which may suppress power grid behavior that may be targeted by cyber attacks. Sandia is presently developing dynamic power models; however, their complexity may pose a barrier to using them with large, complex models of power grids. While the VCSE steady-state model currently works with the IEEE RTS-96 power grid, two other steady-state power grid models (PowerWorld and the Interdependent Energy Infrastructure Simulation System) use models of real power grids.

Economic Models are Limited

The REAcct methodology, which was discussed in the earlier walk-through of the cyber-attack consequence assessment process, is coarse due to the use of limiting assumptions. First, REAcct assumes that economic activity is spatially evenly distributed across a county. For example, if a disruption covers 5 percent of the area of a county and disrupts 50 percent of economic activity, REAcct assumes that 2.5 percent of economic activity is disrupted. However, if the county is sparsely populated, most economic activity could fall within the 5 percent of the county that receives the disruption. In this case, the parameters used by REAcct as inputs should be adjusted to reflect the uneven distribution of economic activity.

Second, REAcct calculates losses in gross regional product and income by assuming that all workers across the country have the same productivity. Data on county employment per industry are multiplied by average national productivity to generate estimates of gross regional product in each county. Because worker productivity varies by county, these estimates contain a degree of inaccuracy.

Third, the REAcct methodology is only valid for interruptions that last from about a week to a month. Depending on the nature of the disrupted asset, only some economic activity in an affected area may be lost. For example, a temporary power outage would not significantly affect businesses that had sufficient backup generation, nor would it significantly impact manufacturers who

can continue to meet demand with on-site or in-transit inventories.

Finally, REAcct assumes little about how the economy will adjust structurally to the disruption which may change the multiplier effects. For example, firms outside the disrupted area may pick up the slack in supply caused by the disruption, former suppliers to the disrupted firms may find new customers, and workers in the disrupted areas may move to find employment. More sophisticated economic models and tools which capture many of these long-term adjustment effects, such as the Regional Economics Models, Inc. (REMI), model, are more appropriate than REAcct for assessing long-term economic consequences that involve structural adjustments.

Extension of The Cyber-Attack-Consequence Assessment Process to other Infrastructures

As previously mentioned, this case study focuses on Sandia's capabilities in carrying out the cyber-attack-consequence assessment process using electric power control systems as an example. The process can be used with other critical infrastructure control systems with modifications to existing capabilities and the addition of infrastructure-impact simulations for new infrastructures.

Of the three steps of the cyber-attack-consequence assessment process focused upon in this case study, the systems-effects step and the infrastructure-impact step need to be modified from the electric power walk-through. For the final step (economic consequence assessment), the REAcct tool can continue to use the same type of infrastructure-disruption scenario as an input (specifications of which counties are affected, how long the disruption lasts, what fraction of their area is affected, and what fraction of economic activity is disrupted), provided that the necessary mappings of infrastructure disruptions to economic disruptions are made. Many of the economic assessment tools that filled the gaps of REAcct are similarly flexible or can include new infrastructures by expanding their models.

System Effect

The process walk-through detailed methods and tools that can currently be used to simulate a cyber attack on an electric power control system and assess the impacts to the electric power grid. Although these tools are tailored to the electric power industry, some tools, such as the VCSE, can be modified to different infrastructures. Other types of physical infrastructure can be simulated by either interfacing existing tools with the VCSE or creating new tools.

Infrastructure Impact

The infrastructure-impact step of the process maps changes in critical infrastructure control systems that are caused by cyber attacks to overall changes in infrastructure. The tools necessary to assess the infrastructure impact of cyber attacks will vary depending on the infrastructure being simulated, especially for infrastructures that have complex interdependencies among components. Thus, models of the specific infrastructure will be useful for developing a detailed and reliable infrastructure-impact scenario that shows how cyber attacks against a control system affect an infrastructure.

Economic Consequence

As mentioned earlier, the economic consequence tools are very flexible and can accommodate a variety of infrastructures, provided that the infrastructure-impact scenario can be mapped to a specific economic disruption. This mapping may be more difficult in infrastructures other than electric power. Most economic activity is highly dependent on electric power, but the same cannot be said for many other infrastructures. For example, a cyber attack on water treatment that resulted in a boil order would likely be more of an inconvenience than an event that halts all economic activity. In the extreme case of an infrastructure impact scenario where all water service was disrupted for a municipality, all economic activity would not be halted; much economic activity does not require water, and there are many common, alternative ways of obtaining water (such as wells).

More detailed economic consequence models, such as the National Infrastructure Simulation and Analysis Center (NISAC-Agent-Based Laboratory for Economics (N-ABLE™)), may be able to better model infrastructure disruptions that lead to more subtle economic disruptions than do interruptions in electric power. Heuristics can be used (or developed) to aid REAcct in mapping an infrastructure disruption to an economic disruption.

6. SOLUTION

The walk-through of the cyber-attack-consequence assessment process earlier in the case study, showed how the process can be easily applied to electric power. There was also an explanation of how some of the gaps in the process for electric power can be closed. Now, let's look at how the two extensions can better integrate the different steps of the process.

The first extension uses probabilistic modeling, which is currently being used for reliability analysis of electric power, to assess economic consequences. The second extension more fully integrates the final three steps of the

process at the software level by interfacing various tools so that the process can be conducted more efficiently.

Probabilistic Modeling

Critical infrastructures consist of complex engineering systems with many components. All of these components can fail, but the failure of individual components does not necessarily mean that the entire system will fail. A system, or parts of the system, is more likely to fail completely when multiple components fail at once.

Probabilistic analysis using the Monte Carlo simulation (An analytical technique in which a large number of simulations are run using random quantities for uncertain variables and looking at the distribution of results to infer which values are most likely. The name comes from the city of Monte Carlo (country of Monaco)), which is known for its casinos.) is often used in reliability engineering to assess the reliability of the system. The most basic simulation assumes that all components fail at random independently of one another. The failure of individual components of a system, can be simulated by assuming a probability distribution for the failure of that component, and drawing random numbers to determine whether the component has failed. For example, the exponential distribution is assumed if it is believed that a component has an equal chance of failing at any given time. Thus, failure of a component could be simulated when a randomly drawn number was below a given threshold during a specific period.

The exponential distribution has one parameter that must be specified for each component. The mean time to failure (MTTF) is, on average, how long a component will operate until it fails. If the recovery time of a component is also assumed to follow the exponential distribution, then another parameter (the mean time to recovery (MTTR)) must also be specified.

At each step, the state of the system is recalculated to reflect failures of individual components. Metrics about the state of the system are recorded. For example, in an electric power grid, the state of a bus (whether or not it is receiving power) could be recorded. After simulating the system for a long time, the recorded metrics can be analyzed to determine overall reliability. Because the Monte Carlo simulation operates over a long time, the results are most useful for determining the long-term costs of failures in the system.

Full Integration of Process Steps/Tools

Finally, a long-term goal may be to fully integrate the system-effect, infrastructure-impact, and economic-consequence steps of the process. Full integration might consist of a single user interface to conduct all three steps simultaneously, by using tools that are interfaced.

The system-effect and infrastructure-impact steps of the process are already interfaced for electric power by using the VCSE. The VCSE simulates the control system, but also interfaces to electric power grid models, which allows it to assess how a cyber attack affects control systems and how those effects propagate throughout the electric power grid. Furthermore, implementation of probabilistic analysis for economic consequences would likely require the infrastructure-impact and economic-consequence steps to be formally integrated so that the Monte Carlo analysis could run quickly.

7. CASE STUDY 3: DEPARTMENT OF HOMELAND SECURITY BATTLE INSIDER THREATS AND MAINTAIN NATIONAL CYBER SECURITY

The U.S. Department of Homeland Security (DHS) is a cabinet department of the U.S. federal government. Founded in 2003, the DHS was created in response to the horrific attacks of September 11th. Its mission is to secure the nation, protect it from terrorist attacks and respond to natural disasters. Headquartered in Washington, D.C., the DHS employs more than 340,000 people who are dedicated to keeping the nation safe. It is the third largest cabinet department, after the Department of Defense and Veterans Affairs, and it has a geographically dispersed network with 21 component agencies.

8. CHALLENGES

The DHS has a vital mission: to secure the nation. At the core of this mission, it was critical that DHS first improve and secure its own infrastructure that supports 21 geographically dispersed component agencies. In 2009, the DHS' Office of the Chief Information Officer, Information Technology Services Office and Risk Management Control Division were faced with the challenge of unifying the 21 component agencies. Their challenge was to strengthen the components through the creation of one secure network and reduce the number of data centers. In order to do this, the DHS needed to coordinate centralized, integrated activities across components that are distinct in their missions and operations. With scores of administrators accessing key critical national infrastructure at these core data centers, the DHS' Risk Management Control Division was tasked with ensuring contained access and monitoring, logging and tracking all administrative changes to its systems. In addition to stringent security policies, the DHS is subject to compliance regulations including Federal Desktop Core Configuration

(FDCC) standards. Launched by the Office of Management and Budget in 2007, the FDCC ensures that federal workstations have standardized, uniform, desktop configurations to enable more consistent and better documented security while reducing costs. The DHS needed a solution that would allow it to support the component consolidation effort, transforming the 21 sites by unifying and controlling access to key servers at those sites while maintaining the separation of duties within and across the component agencies. It also needed a solution that could quickly and easily be dropped into technology already in place. This was a challenging task because the DHS has a wide range of platforms and operating systems, including mainframes, UNIX, LINUX and Microsoft Windows.

9. SOLUTION

The solution criteria were crystal clear. The DHS needed a solution that supported remote access, desktop virtualization, two-factor authentication and auditing. It also needed out-of-the-box multi-platform support along with integration with existing cyber security products. As part of the selection process, the DHS vetted several cyber security products from a variety of market leading vendors. The DHS selected a cyber security product that provides access control for privileged users, including company employees, partners, consultants and IT staff, along with the computing infrastructure. The cyber security product controls, contains and audits the activity of privileged users, whether they originate from inside or outside of the network. The cyber security product also enforces fine grained access control policy on users, contains them to authorized systems and applications, and monitors, logs, records and reports their activities for compliance and security risk management. This gives DHS control over its privileged users and high risk assets. It also allows DHS to enforce access control policies and contains users in a manner that enables them to see only the network resources to which they have access. With an identity-based access control solution, the cyber security product provides the DHS with access control, user containment and audit-quality logging in a single appliance-based offering. From an operations and risk perspective, this allows the DHS to granularly control who gets access to what servers, when and for how long in an easy-to-manage unified offering. The cyber security product also enables DHS to contain users from its 21 sites to authorized systems and applications without any reconfiguration of its network. The cyber security product's capabilities also addressed the DHS requirement to maintain end-to-end accountability.

Finally, the cyber security product has increased security awareness at the DHS. With the cyber security product, the DHS has been able to provide privileged users with highly secure access to key servers in its facilities. As a result, the DHS has increased network security while enforcing the cyber security policy. The DHS has used the cyber security product to maintain Federal Desktop Core Configuration (FDCC) compliance. It does this at the desktop level since the secure access is provisioned via a Web browser without an additional desktop client required. The DHS has also used the cyber security product to streamline operations. This has been possible because the cyber security product provides a single solution for controlling, monitoring, logging and tracking all administrator changes. Now, DHS can easily determine when a change was made and the implications of that change. The DHS derived several additional benefits from the appliance. First, DHS found the anti-leapfrogging capabilities beneficial, which contain users to authorized resources. Another benefit was being able to add keystroke loggers to administrative accounts and prevent them from doing any intentional or unintentional damage.

10. CASE STUDY 4: CYBER SECURITY DEVELOPMENT LIFECYCLE

An employee was about to head home for the weekend from a utility company. Then the company's senior applications system analyst (and go-to computer programmer) heard from site administrators that something was odd with the utility's website. The programmer logged in to the code that controlled the troubled area and found himself staring not at the carefully engineered software he and those in his group helped create, but at a long string of seemingly random numbers and letters. Well, he thought, this can't be good. A quick Web search suggested that the utility's website application software was under attack from something called a botnet, a program built specifically to replicate malicious software on the Web. This particular botnet had an odd name: fringe47. It was spreading rapidly online by injecting itself into vulnerable websites and then waiting for unsuspecting users to click on the site. When they did, the code copied itself on their computers. In a few months, 360,000 sites had been infected. The programmer, who was careful to make sure his own machine wasn't infected as he researched fringe47, eventually found a safe security industry site that gave him enough details about the attack to alert one of his colleagues (manager of information protection at the company) that something was seriously wrong. Word then spread to others on the utility's IT team. Specifically, the code intended to take advantage of a weakness in a database method used to communicate called Structured Query Language, or SQL (pronounced −sequel‖). Fringe47 was diabolically engineered to sniff

out the Achilles heel in SQL. The botnet co-opted an application on the company Website and injected itself directly into a company database. The fear was that in the process, it could get past the utility's larger security perimeter and have its way with the company's software portfolio of applications, database tools and other code. It also had the potential to install itself on the computers of anyone who visited the utility's website. The attack was a legitimate risk to the utility. The immediate question was, could the company's highly sensitive information and processes (including customer billing data and energy trades) be compromised? Just 15 minutes after the programmer's first indication of the cyber attack, the utility had taken down the infected area, a section of the Website that contained news releases and other public relations information.

11. CHALLENGES

SQL injection attacks on corporate software applications are common — and, for victimized companies, the effects range from embarrassment to significant financial losses. Yet at first blush, the cyber attack on the utility seemed fairly innocuous. Fringe47 didn't appear to be causing damage, but it was replicating. The code was not meant to *steal information* from the utility. It was used to *spread the code* to those who came to the website.

The utility did the right thing: To avoid infecting Website users' computers, the company took down the infected pages. Once it did so, the IT staff started dissecting the cyber attack. The programmer and his colleagues identified two internal flaws that had repercussions throughout the utility's software architecture: data validation and improper rights administration.

Data Validation

When visitors came to utility.com looking for a press release, they would input a date to find the document they wanted. As long as they typed in an actual date, everything worked fine. But fringe47 exploited a flaw: Instead of a day, month and year, it inserted a long string of what appeared to be random letters, numbers, and characters. The string was anything but random, however. Because the Website code wasn't designed to validate that the data entered was in a true 8-digit date format, this long, alphanumeric code replaced the original data on the company database with a nefarious computer program.

Improper Rights Administration

Because of the way the site's Web application was originally coded, the requests for press releases were given the right not only to read from (but to write to) the company database. Fringe47 took advantage of these loose privileges to gain access to a part of the utility's information infrastructure. As obvious as this vulnerability sounds now, that wasn't the case when the code was written more than a decade ago. Back then, Web-based attacks were a rarity and the utility had never felt threatened. But, by not updating its application software as cyber criminals got more sophisticated, the company exposed itself to a new generation of risk.

Give Me a Break

In retrospect, the utility got two lucky breaks: First, the original program between the computer that held company data and the one that handled the Web page was set up to limit the time the two could communicate. This so-called, break‖ design, a throwback to the days when data service was slow and expensive, minimized the server's data load. As a result, fringe47 could compromise only the first few rows of the core SQL database before it was cut off. That limited the damage. Second, the utility's corporate communications staff made a habit of going through online press releases once a month to make sure the links still worked. This monthly audit found one that didn't, prompting a call to the IT service desk at the utility, which contacted Website administrators, who tipped off the programmer that something was amiss. As seemingly benign as the cyber attack initially appeared, the utility knew that whoever was behind it was savvy enough to know how to get inside a company – deep inside.

Deja Vu All Over Again

A few months later, an identical cyber attack hit the utility's Website again. The utility had been warned about the vulnerabilities and fixed the vast majority of risks – except for one on a single, long-forgotten page. That was just enough to facilitate a fresh cyber assault. The utility had been stung by yet another outmoded cyber security practice: relying on a checklist approach to security. Prior to the cyber security overhaul, the company started with the traditional process for designing a software product: create lists of what the software would do, lay out how the software would do those tasks, set specific goals for design and other features, and start testing and debugging on the way to a release date.

The company initially took the same approach to dealing with the SQL attack. Once the utility had been flagged about the fringe47 injection, its developers made a list of all potential places they might be exposed, and closed weaknesses one at a time. But they missed one.

It was one single, old Web page that had not been touched in years. But, that second fringe47 attack gave

the utility another clue: The cyber attacker had used a specific type of Google search to pinpoint vulnerabilities with lethal accuracy. Dubbed Google Hacking, by security pros, the technique uses Google's powerful search engine to ferret out weaknesses in Web-based software. This strategy hides the cyber attack from most targets, to the point where Google Hacking victims typically have no clue they're being targeted.

The utility thought it was protected, but it failed to heed one sign: A few years earlier, several third-party security auditors warned the company it was vulnerable to SQL injection attacks. There was some skepticism about the exploitability of these threats. The utility had attempted to secure its applications once before. Seven years earlier, the company started working to improve how it developed new software. But, the commitment to go back in and fix older code was beyond that effort.

Hackers are Way Beyond Smart

Hackers continue to find new avenues of attack. A relatively small group of developers, already extremely busy, now had to find time to find and fix an unknown number of cyber security risks over a vast critical IT infrastructure that supported not only the company website, but every business unit in the company: services like customer care and human resources; applications that run the business like energy trading; and, even how the utility generates and distributes power.

12. SOLUTION

The utility knew it wanted (needed) a new culture for how it engineered, developed and tested its software. It also knew it wanted that culture grounded in widely accepted standards. That way, coders could learn from one another, and the company would not be re-inventing its cultural wheel to make its software more secure. The catch was, no one on staff knew much about how to make applications safer.

The design phase of the cyber security development lifecycle (CSDL) requires developers to create something called a cyber threat model. That is, a sense of the cyber attacks an application *might* face. What kind of exploits might a cyber attacker use? How would hackers gain access to an application running on a computer network? What older, existing pieces of code associated with the new application might be vulnerable? This overall feel for the risks an application might come under allows coders to *anticipate* risks. Threat models need not be complex: Even high-quality ones can be done on the back of cocktail napkins.

Once the standard was set, critical areas were addressed and basic training was completed, next up was spreading the new cyber security culture inside the utility. Two basic lines of work emerged: remediation on the existing code where needed, and maximizing the cyber security of all new code created from that point on. The company-wide remediation was a copy of the early, high-level work on the website: carefully anticipating threats identified by the utility's version of CSDL, analyzing each threat and then refactoring code where necessary. This strategic work was buttressed by scanning tools that helped identify high, medium and low risks. But, despite this automatic assistance, it was immediately clear the work ahead would not be easy.

Time was something the utility's coders had little of. Its IT department was designed to be an internal resource for the coding needs of various departments: providing the company's energy traders with a new way to manage their inventory, helping human resources manage employee benefits, and planning how utilities route their electricity or gas. But, under a mandate from the top, they found a way. And, slowly, cyber software security at the utility moved from afterthought to top-of-mind. Under CSDL, the utility now *started* with cyber security. Step one in the process was identifying a well-thought-out set of cyber threats that showed where a piece of software might be weak. How would the code be used? What was at risk? Then, using its new test tools and protocols, the entire development team became responsible for keeping the code within the standard. The utility had even gone so far as to install a last step — a human review to triple check that all new code cleared the cyber security bar before it went live.

But, the preceding only shows a small piece of what the utility achieved. The company learned that cyber security is *not* an absolute. It is the natural extension of an overall approach to keeping its informational ecosystem immune to cyber attack. Today, the company views cyber security as an evolving issue that forces it to stay ahead of new threats. That means considering cyber security from day one and abandoning a culture of pushing out code as fast as possible.

13. CASE STUDY 5: CYBER SECURITY AND BEYOND . . .. . .

Cyber security is an essential tool for managing risks in today's increasingly dynamic and capable cyber threat landscape. Yet the market for cyber security remains small, and organizations are making only tactical investments in cyber security measures—one of the reasons why there has been an increase in cyber attacks. Evidence suggests that this trend will last for some time to come. However, the anticipation of an increasingly open and mobile enterprise should help refocus the

spotlight on strategic investments in areas like cyber security. Cyber security professionals who wish to see cyber security move up in IT's priority queue should take immediate steps such as demanding secure software from suppliers and requiring rigorous acceptance tests for third-party code to help promote cyber security in the long run.

Because cyber security has a significant impact on vulnerability management, one could infer that the spotlight is only shifting to a different perspective and that commitment to cyber security may not have declined in the final analysis. Although viewed as a priority by many cyber security professionals, cyber security has not seen the appropriate commitment level reflected in IT's budget allocation.

For example, data breaches resulting from web application hacking are almost always accomplished through the exploitation of application vulnerabilities like SQL injection or cross-site scripting. If cyber security is not improved at a larger scale, the industry will continue to be plagued with security incidents that result in data breaches or other consequences that are even more disastrous. Changing the attitude toward cyber security, however, would require a culture shift, a shift that places importance on proactive risk management rather than immediate ROI. This shift won't happen overnight. In the meantime, cyber security professionals should follow these recommendations to implement a few immediate measures to effect positive changes:

- Demand software quality and security from suppliers.
- Perform stringent acceptance tests for third-party code.
- Disable default accounts from applications.
- Establish a secure operational environment for applications.
- Implement effective bug-reporting and handling.

14. CHALLENGES

As the buyer side starts to demand secure cyber software, the power balance will start to shift toward more strategic approaches to managing cyber-level risks. Cyber security professionals can encourage this change by engaging in these longer-term initiatives:

- Work toward an industry certification program for secure development practices.
- Implement a cyber security program.
- Continue to drive awareness of the changing cyber threat landscape.

So, in order to improve cyber security, companies and cyber security professionals should work in a concerted fashion to cultivate a culture that values and promotes cyber security. To help usher in such a culture, cyber security professionals should:

- Do their part to promote a cyber security ecosystem.
- Use mobile proliferation as a catalyst for cyber security.

And Beyond . . ..

Now, let's take quick preview of what cyber security will have to deal with in the near future. Recently, McAfee unearthed a massive, global cyberattack campaign named "Operation Shady RAT" that compromised more than 70 major organizations. Here's what you need to know.

So Where Was DHS When "Operation Shady Rat" Was Alive and Well During the Last 8 Years??

Cybercriminals from China have spent more than six years cautiously working to obtain data from more than 70 government agencies, corporations and non-profit groups. The campaign, named Operation Shady RAT (remote access tool) was discovered by the security firm McAfee.

While most of the targets have removed the malware, the operation persists. The good news: McAfee gained access to a command-and-control server used by the cyber attackers and has been watching, silently. U.S. law enforcement officials are working to shut down the operation. The Chinese government is denying that it sanctioned the cyber attack operation; although, configuration plans for the new DoD F-35 stealth figher were comprised by the cyber attackers. So, with the preceding in mind, the following are five things that came to light:

- Seventy-two (72) organizations were compromised.
- It was just not North America and Europe.
- When the coast was determined to be clear, the cyber attackers struck.
- This was a single operation by a single group (probably the Chinese).
- The only organizations that are exempt from this cyber threat were those that didn't have anything valuable or interesting worth stealing, from a national security point of view.

The loss of this data represents a massive economic cyber threat not just to individual companies and industries, but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape; the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world; not to mention, the national security impact of the loss of sensitive intelligence or defense information.

Yet, the public (and often the industry) understanding of this significant national cyber security threat is largely minimal due to the very limited number of voluntary disclosures by victims of intrusion activity compared to the actual number of compromises that take place. With the goal of raising the level of public awareness today, this is not a new cyber attack, and the vast majority of the victims have long since remediated these specific infections. Although, whether most victims realized the seriousness of the intrusion or simply cleaned up the infected machine without further analysis into the data loss remains an open question.

The actual intrusion activity may have begun well before 2006, but that is the earliest evidence that was found for the start of the compromises. The compromises themselves were standard procedure for these types of targeted intrusions: a spear-phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit when opened on an unpatched system will trigger a download of the implant malware. That malware will execute and initiate a backdoor communication channel to the web server and interpret the instructions encoded in the hidden comments embedded in the webpage code. This will be quickly followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and move laterally within the organization to establish new persistent footholds via additional compromised machines running implant malware; as well as, targeting for quick exfiltration the key data that the cyber attackers came for. In the end, one very critical question remains unanswered: Why wasn't the Department of Homeland Security (DHS) all over this cyber breach during the last 6 years when "Operation Shady Rat" was alive and well?? After all, isn't DHS supposed to be the security guardians of the cyber world?

If "Operation Shady Rat," wasn't bad enough, hackers are now using outfitted model planes/drones to hack into your wireless system. Built from an old Air Force target drone, the Wireless Aerial Surveillance Platform (WASP) packs a lot of technological power into a flying high-end cyber endurance package.

Could it Get any Worse: Use of Model Planes/ Drones to Hack into Wireless Systems

Built with a tiny on-board computer (Linux powered, natch), the WASP is bristling with hacking tools, along with a custom-built 340 million word dictionary for brute-forcing passwords, the BackTrack suite (BackTrack provides users with easy access to a comprehensive and large collection of security-related tools ranging from port scanners to password crackers.), a 4 G T-Mobile card, an HD camera, and 32 GB onboard storage. Just what does WASP do with those gigabytes? Originally, it was designed for Wi-Fi penetration — cracking network passwords while loitering above a target area. But, the newly upgraded WASP can now trick GSM phones into connecting with its 4 G card as if it were a standard cell-phone tower. Once connected, the WASP quietly records any phone conversations or text messages while connecting the call via VOIP, thus giving the mark the impression that the call went through normally.

Keep in mind that nothing on the WASP is particularly new. The password cracking techniques have been around for quite some time, and the phone-spoof is based off a trick shown off at Defcon in 2010. But, by placing them on a flying platform, consumer technology and hacking techniques have progressed to the point where once untouchable targets are now vulnerable.

If "Operation Shady Rat," and "WASP" weren't bad enough, hackers are now targeting security companies. Recently, a band of Internet vigilantes calling itself Anonymous (17 of whom were recently arrested by FBI raids), had sneaked into several security companies' computers to demonstrate those companies' insecurity.

Worse and Worser: Cyber Security Guardians are Now Hacker Targets

Recently, several security firms and consultants have been hit by the cyber intruders they are hired to keep at bay. The group, calling itself Anonymous, released internal company documents from those security firms.

The security firms and consultants are hired to protect corporate and government data, including the most confidential intelligence information, across a vast virtual frontier. The string of embarrassing cyber attacks on them demonstrates how vulnerable everyone is online, including those who are paid to be the protectors.

Other cyber attackers are mysterious and more worrying entities than the Anonymous group; as in the case of the still unknown organization (probably Chinese) that recently breached the systems of RSA, whose electronic security tokens are used across many industries. The cyber hackers used information obtained in the RSA cyber attack to break into Lockheed Martin, the largest military contractor in the country.

Anonymous, for its part, has made it plain that it goes after defense and intelligence contractors to expose their security vulnerabilities, not for financial or strategic gain. Booz Allen Hamilton, a company based in McLean, Va. (that does computer security work for the Defense Department), was also hit by the group. The cyber hackers released the e-mail addresses of over 100,000 military personnel.

The most notorious breach of a security company came after an executive at HBGary Federal, a relatively

small consultant eyeing a government contract, boasted publicly of his ability to unmask the members of Anonymous. In response, hackers made off with a large trove of the company's e-mail messages and dumped them online, exposing details of its business transactions.

The spate of cyber attacks (and the fear of more) could actually end up buoying the fortunes of the global cyber security industry. All of the major defense and intelligence contractors have expanded their digital cyber security wings in recent years. They are simply following the money.

For better or worse, securing the Internet has been largely left to private players. Even government information, is increasingly guarded by private companies, whose actions can be difficult to monitor and hold accountable.

Finally, speaking of worse, the group known as Anonymous has struck again! Recently, the cyber hacker group hacked into some 80 mostly rural law enforcement websites in the United States, a data breach that leaked sensitive information about ongoing investigations. The cases have now been compromised, and may be thrown out.

Revenge of Anonymous

The loose-knit international cyber hacking collective known as Anonymous, posted a cache of data to the Internet, including emails stolen from officers, tips which appeared to come from members of the public, credit card numbers and other information. Anonymous claimed that it had stolen 20 gigabytes worth of data in retaliation for arrests of its sympathizers in the U.S. and Britain.

Though many of the leaked emails appeared benign, some of the stolen material carried sensitive information, including tips about suspected crimes, profiles of gang members and cyber security training. The emails were mainly from sheriffs' offices in Arkansas, Kansas, Louisiana, Missouri and Mississippi.

Anonymous did not specify why these sheriffs' departments were targeted. But, Anonymous members have increasingly been pursued by law enforcement in the United States and elsewhere following a string of high-profile data thefts and denial of service attacks — operations that block websites by flooding them with traffic.

Recently, the FBI and British and Dutch officials, made 32 arrests. Many of the arrests related to the group's attacks on Internet payment provider PayPal Inc., which has been targeted over its refusal to process donations to WikiLeaks. The group also claims credit for disrupting the websites of Visa and MasterCard, when the credit card companies stopped processing donations to WikiLeaks and its founder, Julian Assange.