EVALUATION

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks

This is a revised version of the report prepared for public release.

In recognition of Secretarial Order No. 3380, we are providing estimated costs associated with certain work products. Applying a formula involving prior salary and benefit expenses, we estimate the cost of preparing this report to be $254,000.

Report No.: 2018-ITA-020 September 2020

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Memorandum

SEP 1 4 2020

To: William E. Vajda
Chief Information Officer

From: Mark Lee Greenblatt
Inspector General

Subject: Final Evaluation Report – *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks*
Report No. 2018-ITA-020

This memorandum transmits our evaluation report on the security of the U.S. Department of the Interior's wireless networks. We found that the Department did not deploy and operate a secure wireless network infrastructure. Specifically, the Department's wireless network policy did not ensure bureaus kept inventories of their wireless networks, enforce strong user authentication measures, require periodic tests of network security, or require network monitoring to detect and repel well-known attacks. The Office of the Chief Information Officer (OCIO) and the bureaus promptly responded to our findings upon notification. We made 14 recommendations to strengthen the Department's wireless network security to prevent potential security breaches, which could have a severe adverse effect on Department operations, assets, or individuals.

In response to our draft report, the Department concurred with our 14 recommendations and provided information on actions taken and planned, responsible officials, and target dates for completion. Based on the Department's response, we consider 13 recommendations resolved but not implemented and 1 recommendation unresolved. We met with the OCIO to discuss our concerns about its proposed solution for the unresolved recommendation and additional steps that may be taken to more effectively secure the Department's infrastructure in the event a wireless network breach occurs. Based on those discussions, we clarified this recommendation in the report. We will refer the 13 unimplemented recommendations to the Office of Policy, Management and Budget (PMB) for implementation tracking and the single unresolved recommendation to the PMB for resolution.

We appreciate the Department's cooperation during this evaluation and its willingness to engage with our office at all stages of the process. If you have any questions about this report, please contact me at 202-208-5745.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

Contents

Results in Brief

The U.S. Department of the Interior operates hundreds of wireless networks to allow employees greater flexibility in mobile computing. Wireless networks are much easier to attack and potentially compromise than their wired counterparts because they are often accessible from public areas. Physical security controls such as guards and locked or gated entries will not prevent an attacker from attempting to eavesdrop on wireless communications or gain unauthorized access to the Department's internal or wired networks. Thus, it is imperative that the Department's wireless networks be securely configured, regularly tested, and continuously monitored to detect and repel wireless network attacks.

Our evaluation revealed that the Department did not deploy and operate a secure wireless network infrastructure, as required by the National Institute of Standards and Technology (NIST) guidance and industry best practices. We conducted reconnaissance and penetration testing of wireless networks representing each bureau and office. To do this, we assembled portable test units for less than $200 that were easily concealed in a backpack or purse and operated these units with smartphones from publicly accessible areas and locations open to visitors. Our attacks simulated the techniques of malicious actors attempting to break into departmental wireless networks, such as eavesdropping, evil twin, and password cracking.

These attacks—which went undetected by security guards and IT security staff as we explored Department facilities—were highly successful. In fact, we intercepted and decrypted wireless network traffic in multiple bureaus. Even worse, with regard to two bureaus, our penetration test went far beyond the wireless network at issue and gained access to their internal networks. In addition, we successfully obtained the credentials of a bureau IT employee and were able to use that person's credentials to log into the bureau's help desk ticketing system and view the list of tickets assigned to the employee.

These are not speculative or academic concerns; to the contrary, as we noted above, we used the same tools, techniques, and practices that malicious actors use to eavesdrop on communications and gain unauthorized access. Many of the attacks we conducted were previously used by Russian intelligence agents around the world, as outlined in a 2018 U.S. Department of Justice indictment. [1]

Not only did our attacks reveal that the Department did not deploy and operate a secure wireless network infrastructure, we also found that several bureaus and offices did not implement measures to limit the potential adverse effect of breaching a wireless network. Because the bureaus did not have such protective measures in place, such as network segmentation, we were able to identify assets containing sensitive data or supporting mission-critical operations. Further, we found that the Department:

- Did not require regular testing of network security

- Did not maintain complete inventories of its wireless networks

[1] https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

- Published contradictory, outdated, and incomplete guidance

These deficiencies occurred because the Office of the Chief Information Officer (OCIO) did not provide effective leadership and guidance to the Department and failed to establish and enforce wireless security practices in accordance with NIST guidance and recommended best practices. Without operating secure wireless networks that include boundary controls between networks and active monitoring, the Department is vulnerable to the breach of a high-value IT asset, which could cripple Department operations and result in the loss of highly sensitive data.

We make 14 recommendations to strengthen the Department’s wireless network security to prevent potential security breaches, which could have a severe adverse effect on Department operations, assets, or individuals. The OCIO and the bureaus promptly responded to our findings upon notification. In response to our draft report, the OCIO concurred with all 14 recommendations and stated that it is working to implement them. As described subsequently, 13 of the 14 recommendations are resolved, and one is still unresolved.

Introduction

Objective

Our objective was to determine whether the U.S. Department of the Interior deployed and operated a secure wireless network infrastructure across its bureaus in accordance with National Institute of Standards and Technology (NIST) guidance and industry best practices.

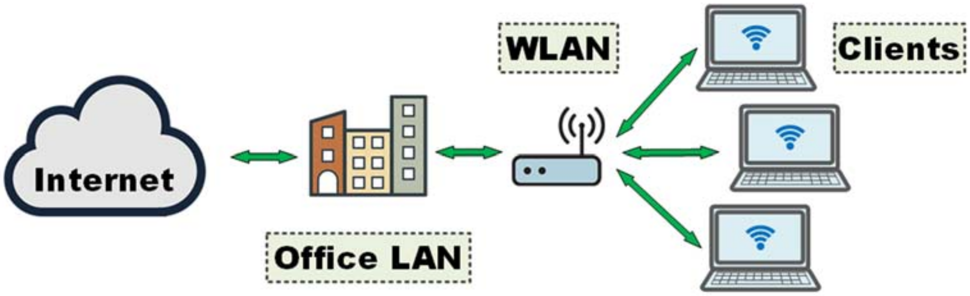
The scope and methodology for this evaluation can be found in Appendix 1.

Background

Wireless computer networks enable users to access the internet or an organization’s internal computer systems and data without physical connections, such as network or peripheral cabling. Key components of wireless network infrastructure include wireless access points, repeaters, and bridges that connect computing devices to the internet or to an organization’s internal computer networks. Users connect to wireless networks with “client devices” such as laptops, smartphones, and tablets. The client device uses encoded credentials consisting of either a pre-shared key or a username and password to prove its identity and gain access to the network (the process is called authentication). There are different types of wireless network authentication with different ways of encoding credentials, but for simplicity we will refer to all types as “encoded credentials.”

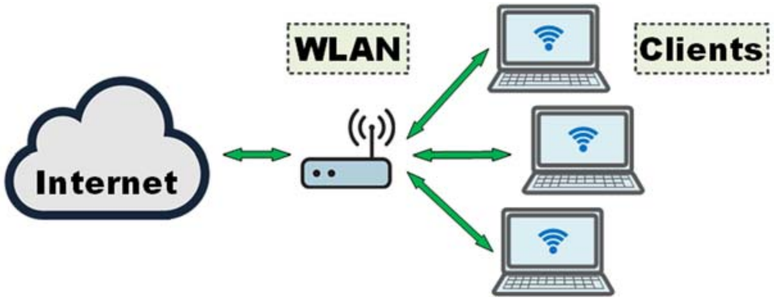
Wireless networks exchange data via radio communications and operate over a limited geographic area such as an office complex or building. Wireless networks are commonly implemented as either an extension of an organization’s wired or internal network (see Figure 1) or as a standalone network (see Figure 2) to provide users with internet access.

Figure 1. A Wireless Network as an Extension of an Internal Network



Source: OIG illustration created using Shutterstock images.

Figure 2. A Standalone Network



Source: OIG illustration created using Shutterstock images.

While wireless networks allow for greater flexibility in mobile computing, they are targeted by malicious actors to eavesdrop on communications. Moreover, if the wireless network is an extension of the organization's internal computer networks, attackers may gain unauthorized access to an organization's internal networks by exploiting wireless network vulnerabilities. It is imperative that wireless networks be configured and maintained according to secure standards to maintain confidentiality of communications and prevent unauthorized network access.

Wireless Network Attacks and Testing Techniques

Before a laptop or smartphone can access data from a wireless network, the device must authenticate to the wireless access point. The two most common types of wireless authentication are (1) group authentication, in which users associate to an access point using the same pre-shared key, or (2) individual authentication, in which each user has a unique user ID and password. Group authentication is inexpensive, easy to implement, and commonly used for home or guest wireless networks. Sharing passwords is considered a hazardous practice in large organizations, however, so individual authentication is often preferred depending on the resources and data available to the clients. Both types of authentication methods encode the credentials during transmission to prevent an attacker from reusing them upon discovery.

In order to test how these credentials were being protected from eavesdroppers, we built handheld wireless attack test units that we could operate while exploring departmental facilities. We used low-cost hardware and open-source software, such as Raspberry Pi[2] single board computers and Kali Linux[3] to build our test units. We used smart phones to inconspicuously control the test units. We also required windows of opportunity in order to be successful—namely, we needed to get the devices physically close enough to communicate with devices on the network, as well as clients to be connected to or in the process of connecting to the network. With a short schedule of visits, our test results were constrained by these opportunities.

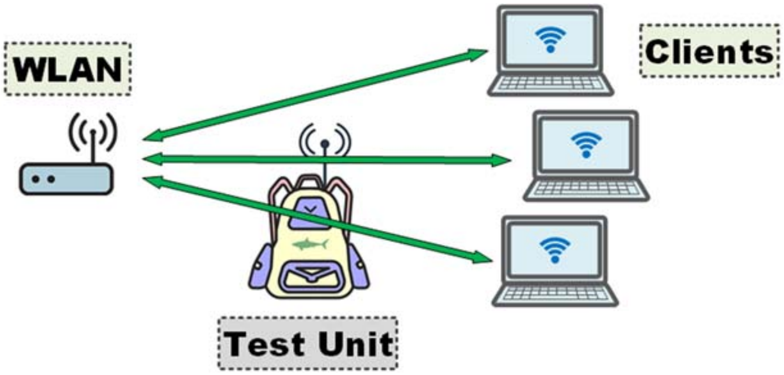
Below we describe two of the network attack techniques we tested in this evaluation: capturing pre-shared keys from a wireless network and capturing unique user credentials from a wireless network.

[2] https://www.raspberrypi.org/
[3] https://www.kali.org/

Capturing Pre-Shared Keys From a Wireless Network

To capture pre-shared keys, an attacker first uses inexpensive and easily available tools to eavesdrop on the wireless network traffic between a client and an access point, waiting for traffic that includes the encoded credentials (see Figure 3). After collecting encoded credentials, the attacker attempts to break the encoding and recover the credentials in clear text. For simple pre-shared keys of low complexity (e.g., dictionary words, short in length), the attacker may be able to quickly break the encoding using the same equipment used to capture it. If not, the encoded credentials can be transmitted to higher performance remote systems where additional efforts could be dedicated to breaking the encoding. If the attacker successfully breaks the encoding, it can then use the recovered credentials to eavesdrop on communications, gain unauthorized access to the network, or gain unauthorized access to other systems inside of the network.

Figure 3. Wireless Test Units Eavesdrop on Wireless Networks and Record Encoded Credentials



Source: OIG illustration created using Shutterstock images.

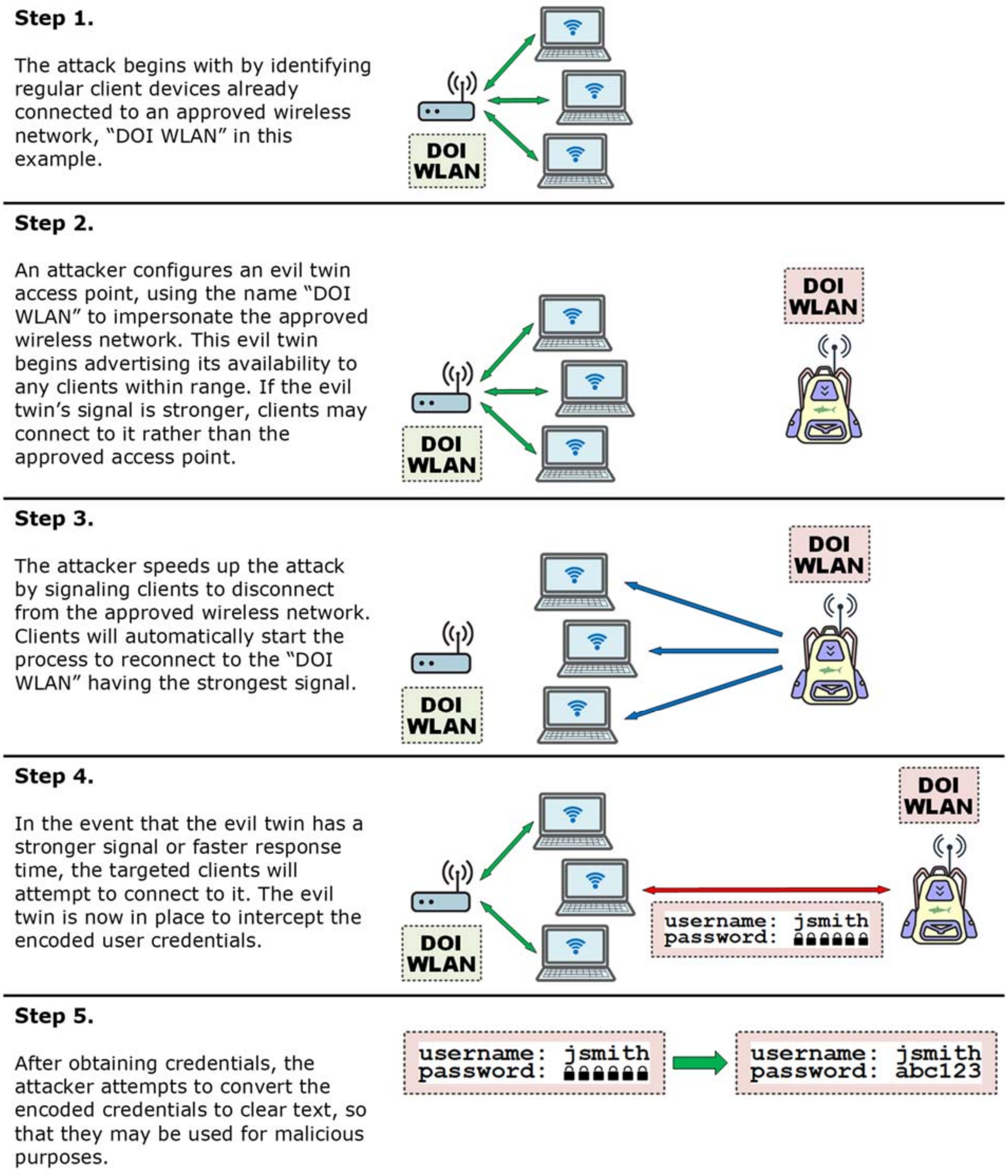
There is no control that can prevent an attacker from passively collecting wireless network traffic from a publicly accessible area and then attempting to recover the pre-shared key. Regularly changing pre-shared keys and requiring they be of significant length and complexity will reduce the likelihood that an attacker will be able to break the encoding and recover clear text credentials.

Capturing Unique User Credentials With an Evil Twin Access Point

An evil twin attack exploits a fundamental weakness in wireless security—client devices do not distinguish between two access points broadcasting the same wireless network name. To capture user credentials, an attacker configures a malicious wireless access point to impersonate a vulnerable wireless network that a client device would normally connect to. This is commonly referred to as an “evil twin attack.”

To speed up the attack, commands can be broadcast to client devices and access points to force them to reauthenticate. This can cause the client to connect to the evil twin network and transmit encoded credentials. If encoded credentials are captured when a client connects, the attacker attempts to break the encoding to recover the user credentials in clear text. See Figure 4 for a diagram of an evil twin attack.

Figure 4. Execution of an Evil Twin Attack



Step 1.

The attack begins with by identifying regular client devices already connected to an approved wireless network, "DOI WLAN" in this example.

Step 2.

An attacker configures an evil twin access point, using the name "DOI WLAN" to impersonate the approved wireless network. This evil twin begins advertising its availability to any clients within range. If the evil twin's signal is stronger, clients may connect to it rather than the approved access point.

Step 3.

The attacker speeds up the attack by signaling clients to disconnect from the approved wireless network. Clients will automatically start the process to reconnect to the "DOI WLAN" having the strongest signal.

Step 4.

In the event that the evil twin has a stronger signal or faster response time, the targeted clients will attempt to connect to it. The evil twin is now in place to intercept the encoded user credentials.

username: jsmith
password: 🔒🔒🔒🔒🔒🔒

Step 5.

After obtaining credentials, the attacker attempts to convert the encoded credentials to clear text, so that they may be used for malicious purposes.

username: jsmith
password: 🔒🔒🔒🔒🔒🔒

username: jsmith
password: abc123

Source: OIG illustration created using Shutterstock images.

Other wireless network attacks can be used in conjunction with an evil twin attack to collect user credentials in clear text, eliminating the need for an attacker to spend time attempting to break the encoded credentials.

Once attackers obtain clear text credentials, they can use them to gain unauthorized access to the organization's computer networks to steal sensitive data, disrupt operations, or establish a foothold on the target for future exploitation. Mutual client device and access point authentication using digital certificates are an effective countermeasure against the evil twin attack. This additional security measure prevents client devices from authenticating to an evil twin access point.

Findings

We found that that the Department did not deploy and operate a secure wireless network infrastructure. For instance, we found that four bureaus operated wireless networks that were vulnerable to evil twin attacks; in fact, we conducted a successful evil twin attack that intercepted user credentials, which we then used to access two bureaus' internal networks. Our six findings are based on an overall program review and technical testing of the Department's wireless network infrastructure.

The Department's contradictory and outdated guidance, incomplete inventory, and lack of technical security testing led to its implementation of insecure wireless networks. We exploited vulnerabilities in the protocols used to authenticate individuals using unique user credentials and those using pre-shared keys. In addition, we gained more access than necessary because the Department did not follow the principle of least privilege[4] and did not have the proper defense-in-depth[5] security controls.

We conducted reconnaissance and penetration testing of wireless networks at 91 locations representing each bureau and office. Using the same tools, techniques, and practices employed by hackers to eavesdrop on communications and gain unauthorized access, we successfully intercepted and decrypted wireless network traffic and gained access to two bureaus' internal networks by exploiting wireless network vulnerabilities. We accessed the Department's Enterprise Services Network (ESN) through the bureau wireless networks we compromised. The ESN networking infrastructure supports communication between bureaus, offices, the Department, and the internet.

Wireless Networks Breached Using Evil Twin Attacks

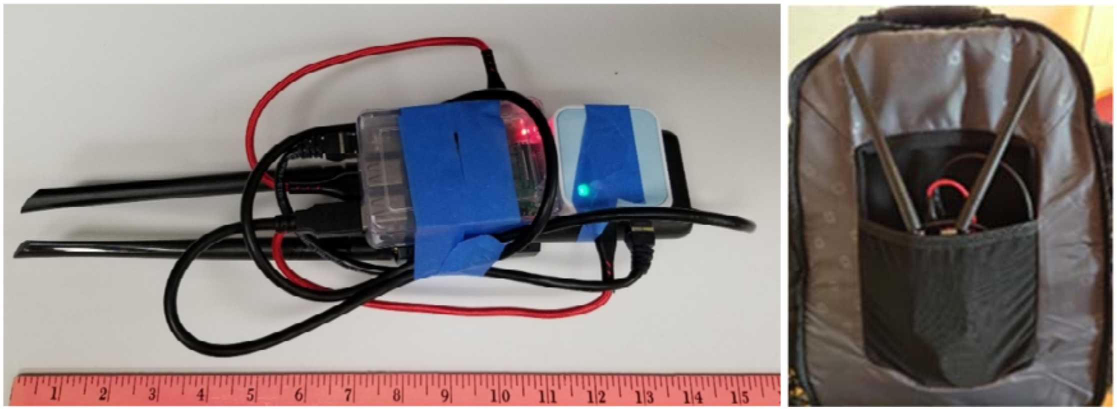
We found that four bureaus operated wireless networks that were vulnerable to evil twin attacks. We successfully executed an evil twin attack to obtain user credentials from two bureaus' networks and used the stolen credentials to access these bureau wireless networks. The bureau wireless networks we compromised were extensions of their internal computer networks; therefore, our attack into the wireless networks allowed us to gain access to their internal networks.

We built our wireless test units for less than $200 each. We brought the equipment, concealed in backpacks (see Figure 5), to publicly accessible areas of bureau facilities. We used a smartphone to inconspicuously control the test units. These attacks went undetected by security guards at the different locations as well as by IT staff responsible for detecting attacks against the Department's computer networks.

[4] The principle of least privilege is that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. Source: https://csrc.nist.gov/glossary/term/least-privilege.

[5] Defense-in-depth is a cybersecurity risk management strategy that involves implementing multiple layers of security with the intention of limiting the impact in the event of a successful attack. Source: https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth.

Figure 5: Our Assembled Wireless Test Units Were Easily Hidden in a Backpack

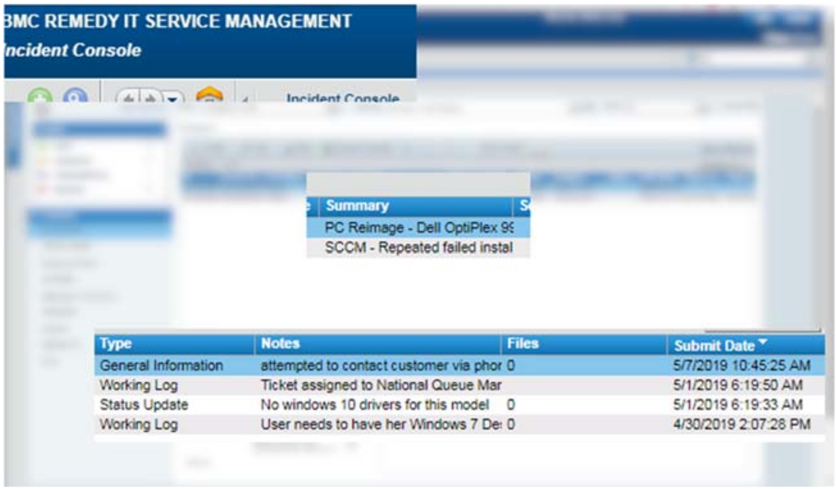


We collected five sets of encoded credentials and recovered two of them into clear text for our own use. We were 40 percent successful in recovering encoded credentials to clear text due to weak passwords. Layering additional wireless authentication attacks with an evil twin attack allowed us to collect two more credentials in clear text without the need for additional steps and computing to break the encoding.

We used the recovered credentials to perform internal reconnaissance scans against the Department's internal networks. We also tested the credentials to determine whether they provided access to additional systems beyond just wireless networks. One set of credentials belonged to a bureau IT specialist. We used these credentials to sign into the bureau's help desk ticketing system and view the list of tickets assigned to the individual (see Figure 6). Help desk systems contain sensitive information such as network architecture and system vulnerabilities. Attackers could use this access to enhance their attacks against the Department's networks.

> In short, our successful evil twin attacks and offline credential analysis obtained passwords 40 percent of the time. When we coupled a successful evil twin attack with additional wireless authentication attacks, we successfully obtained clear text passwords every single time. This removed the need for any offline credential analysis.

Figure 6: Help Desk Tickets Assigned to a Department IT Specialist



Summary
PC Reimage - Dell OptiPlex 9ç
SCCM - Repeated failed instal

Type	Notes	Files	Submit Date
General Information	attempted to contact customer via phor	0	5/7/2019 10:45:25 AM
Working Log	Ticket assigned to National Queue Mar		5/1/2019 6:19:50 AM
Status Update	No windows 10 drivers for this model	0	5/1/2019 6:19:33 AM
Working Log	User needs to have her Windows 7 De:	0	4/30/2019 2:07:28 PM

Our attacks succeeded because the vulnerable bureaus failed to follow best practices for configuring their wireless networks. Specifically, NIST Special Publication 800-97, *Establishing Wireless Robust Security Networks* (SP 800-97)[6], recommends Federal agencies implement mutual client and access point authentication using digital certificates. This additional security measure prevents client devices from authenticating to an evil twin. If the Department had followed NIST SP 800-97 recommendations, the bureau wireless networks we tested would not have been vulnerable to our evil twin attack.

Bureau Responses

Due to the significant impact this weakness introduced, one bureau shut down its enterprisewide wireless infrastructure for 3 weeks. The bureau requested that we test and validate its resolution before it restored services. Similarly, another bureau requested a detailed briefing where we demonstrated the weakness and reviewed its plans to resolve the issue. We consider these responses to be effective and timely.

A third bureau responded to our findings by restricting access to internal resources from the breached wireless network. The only resource left available was internet access. According to the bureau, this forced the clients of that wireless network to use VPN (virtual private network) connections to access internal resources. While this protects the traffic from eavesdropping and direct network access via that wireless network, credentials can still be collected and compromised for use elsewhere. It is unclear if the bureau enforced these restrictions for all its wireless networks because the bureau did not centrally manage them and did not document them in its wireless inventory. We consider this response to be ineffective.

In response to our findings, a fourth bureau stated that it began migrating to a combination of the OCIO's more secure wireless network, where available, and a new internal wireless infrastructure, which we did not test. The bureau left its insecure networks operating during the transition. At the conclusion of our evaluation, the bureau had not yet completed its transition,

[6] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

and we were unable to validate the solution. We consider this response to be unnecessarily risky and ineffective.

Recommendation

We recommend that the OCIO:

1. Require and enforce the use of mutual certificate authentication (client and server) for all ESN connected networks, specifically prohibiting pre-shared key authentication for ESN connected networks

Pre-Shared Key Authentication Left the Department Vulnerable to Eavesdropping

During our site visits, we used our wireless test units to perform eavesdropping attacks on wireless networks utilizing pre-shared keys for client authentication. We compromised four wireless networks at two bureaus and one office that used pre-shared keys. While the DOI denied ownership of any wireless networks, we were not confident in its response due to the signal strength in relationship to our position as we explored the facility. Network operators at the two bureaus confirmed that their wireless networks were standalone networks used to provide internet access and were not connected to any bureau wired networks.

NIST SP 800-97 recommends that organizations not implement group authentication such as pre-shared keys on wireless networks due to heightened risk posed by eavesdropping attacks. Pre-shared keys are shared passwords used to authenticate to the wireless network. Because the Department did not expressly prohibit the use of pre-shared key authentication for all networks, some bureaus operated this type of network.

As part of our testing, we collected encoded credentials for 14 additional wireless networks that used pre-shared keys. We were unable to compromise those networks as we could not break the pre-shared keys in the time allotted to our evaluation. However, given more time, we may have compromised more of these networks because pre-shared keys are rarely changed.

If the pre-shared key for these networks or any we did not identify is discovered, a malicious actor could easily eavesdrop on all clients of the wireless network because the same pre-shared key is used to encrypt communications for all wireless users. The resulting opportunity for attackers to simultaneously eavesdrop on multiple confidential employee communications greatly magnifies the potential adverse effects of a security breach of a wireless network using pre-shared key authentication. Strong pre-shared keys coupled with an additional layer of security, such as a VPN, would reduce the eavesdropping risk at offices with a need to operate this type of network.

Recommendation

We recommend that the OCIO:

2. Require an additional layer of encryption not provided by the wireless network for any official use of non-ESN connected networks that use pre-shared key authentication, such as forced VPN connections

Lack of Network Segmentation Increased Risk to the Department

Compounding the impact from the evil twin finding, we found that the Department and bureaus failed to implement widely recommended defense-in-depth measures, such as network segmentation, to limit the potential adverse Departmentwide effect of a breach to a bureau wireless network. We connected to bureau networks using the credentials we compromised with the evil twin attack and enumerated[7] high-value IT assets. Network isolation is a key defense-in-depth control that can limit the adverse effects of a successful cyber attack.

We previously reported network isolation findings to the Department. As noted in our 2016 evaluation, *Interior Incident Response Program Calls for Improvement*:[8]

> In the recent past, the OCIO desegregated the bureaus' networks to improve service delivery, resulting in the widespread removal of internal security segmentation and monitoring programs, such as firewalls and intrusion detection systems. This focus on improving service delivery across bureau and facility boundaries came with the consequence of weakened security. This significantly increased risk to the Department's IT assets by making it easier to access these systems without security monitoring. A network without security segmentation is commonly referred to as a flat network.

Without network segmentation, an attacker, once inside a bureau's network, can pivot to other bureaus and their computer networks without restriction or detection. Credentials collected by evil twin attacks can be used to grant further access to Department and bureau systems. The attacker can then attempt to steal sensitive data, disrupt operations, or establish a foothold for future exploitation.

[7] Network Enumeration is the process of identifying systems that are both online and responding to network traffic. This process can also identify the system type, software, and services that are available.

[8] https://www.doioig.gov/reports/interior-incident-response-program-calls-improvement

Recommendation
We recommend that the OCIO: 3. Implement network segmentation to isolate clients connected to bureau wireless networks from accessing unrequired resources at other bureaus

The OCIO Failed To Provide Effective Oversight and Guidance

The OCIO failed to provide bureaus and offices with the effective oversight and guidance required to implement a secure wireless infrastructure program. Specifically, we found that the OCIO:

- Did not conduct or require wireless network security testing or monitoring
- Had incomplete wireless network inventories
- Published contradictory, outdated, and incomplete guidance

The OCIO is responsible for all IT management, including wireless networks, per the August 15, 2016 Secretarial Order No. 3340, *Strengthening and Securing Information Management and Technology at the Department of the Interior.* This secretarial order brings the Department in line with the Federal Information Technology Acquisition Reform Act (FITARA) and establishes that the Department's Chief Information Officer (CIO) will be responsible for the oversight and management of all information management and technology within the Department.

Lack of Wireless Network Security Testing or Monitoring

We found that the Department, bureaus, and offices did not perform periodic security testing of their wireless networks or monitor the networks for malicious activity. NIST Special Publication 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems*[9] (SP 800-53) sets forth multiple security controls to be implemented within agency information systems. Control *CA-2 Security Assessments*[10] defines the need for agencies to conduct regular independent assessments of selected security controls in IT systems having a security categorization (under NIST FIPS 199[11]) of moderate or high impact. The wireless networks we tested were categorized as moderate impact, and many were directly connected to the ESN, which the Department categorized as high. According to FIPS 199, a security breach of a moderate impact IT system can be expected to have a serious adverse effect on the organization's operations, assets, or individuals.

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[10] https://nvd.nist.gov/800-53/Rev4/control/CA-2

[11] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

NIST Special Publication 800-153, *Guidelines for Securing Wireless Local Area Networks*[12] (SP 800-153), recommends conducting assessments of the overall security of wireless networks at least annually. The SP 800-153 also recommends performing periodic security assessments at least quarterly unless a continuous monitoring platform is in place to collect and report on wireless network attacks and vulnerabilities.

Although the Department conducted annual security control assessments, we found that it did not include wireless network security in these assessments. The OCIO as well as the contractors responsible for the OCIO's wireless network informed us during separate interviews that they did not perform security testing on wireless networks. The only testing they reported was designed to gauge usability and performance. The OCIO told us that it relied solely on the assurances of the Assistant Chief Information Security Officers (ACISO) that their bureaus and offices were securely operating wireless network infrastructures in accordance with Department security standards.

We asked each bureau ACISO to identify any technical testing performed between July 2016 and 2019. Beyond usability and performance testing similar to what was conducted by the OCIO and its contractors, only one bureau's response included security testing. The bureau contracted an independent assessment, which included a penetration test of its wireless networks in 2017.

Performing wireless security testing as part of its annual security control assessments would have provided the Department with the opportunity to identify and mitigate the weaknesses we exploited prior to our evaluation. This is borne out by the fact that the single security test performed by one of the bureaus we successfully compromised identified the same evil twin vulnerability and made similar recommendations as made in this report.

> While our attacks required physical access to Department and bureau facilities, the OCIO did not consider the physical presence of an attacker inside of a Department facility to be a "successful" attack and did not investigate.

NIST SP 800-153 recommends continuously monitoring all wireless networks for well-known attacks, including the types of attacks we used in our testing. Some of our tests generated alerts in Department and bureau wireless intrusion detection systems, but the incident responders did not treat our attacks as potentially malicious.

In our 2016 report (Report No. 2016-ITA-020), we recommended that the OCIO "Develop a dedicated group of incident responders to perform threat hunting and containment activities." Four years later, this recommendation remains open. Had this been completed, a team of individuals dedicated to looking for the types of attacks we performed may have been able to detect and respond our attacks.

[12] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

Recommendations

We recommend that the OCIO:

4. Perform periodic audits and penetration testing of wireless networks, regardless of security categorization

5. Establish a standard operating procedure that defines indicators of malicious wireless activity and defines when and how to perform and record investigations of those activities

6. Establish an SOP to treat evil twin alerts as a high-level threat

7. Establish an SOP to implement a wireless intrusion prevention system to suppress suspected evil twin attacks

8. Include wireless infrastructure when developing dedicated group of incident responders to perform threat hunting and containment activities (building on Recommendation 11 from Report No. 2016-ITA-020)

Incomplete Wireless Network Inventories

We found that bureaus and offices did not maintain a complete and accurate inventory of their wireless networks. The NIST SP 800-53 control CM-8, *Information System Component Inventory*, requires that Federal agencies develop and maintain inventories of their information system components, including wireless networks.[13] As part of our evaluation, we asked the OCIO to provide a Departmentwide list of wireless networks by bureau and office. The OCIO worked with bureaus and offices to compile a list of wireless networks; however, we found that the list provided was incomplete. The Office of the Chief Information Officer (OCIO) relied heavily on bureau self-reporting of wireless network inventories and did not validate those inventories.

We were unable to perform additional planned tests due to the lack of a reliable inventory. We were also limited in our ability to focus our testing on high-risk networks. We had to rely on a list of approximately 2,200 locations of the Department's wired networks (provided by the Department's IT services provider) to select sites for testing. Using an inventory of wired connections meant that we had no way of knowing whether the sites we selected and visited operated wireless networks until we were on site at each location. We selected 91 sites, in major metropolitan areas for wireless network security testing. All of the Department's bureaus and offices were represented in our sample.

As part of our site visits, we developed lists of wireless networks we discovered through our technical testing. We identified 34 wireless networks that were not included in the wireless network inventory provided by the OCIO. We confirmed that 26 of the 34 wireless networks

[13] https://nvd.nist.gov/800-53/Rev4/control/CM-8

were authorized, meaning they belonged to a bureau or office. The remaining eight wireless networks were unaccounted for and may be the result of rogue access points[14] installed by local facilities. We based this conclusion on the following characteristics:

- Network name matching bureau or office wireless network naming conventions
- Network name that included the facility name or street address
- Network name belonging to a decommissioned wireless network
- High signal strength

The presence of wireless networks that are accessible from Department offices and broadcasting network names like those of approved Department wireless networks is troubling. The fact that the Department could not account for these networks increases the risk that rogue wireless networks may have been deployed. Monitoring for rogue wireless networks is impossible, however, without a complete inventory of approved wireless networks. In addition, the Department's ability to securely configure, test, and monitor authorized wireless networks is also impossible without a complete wireless network inventory. In 2017, the OCIO mandated a limit of approved wireless networks to one per Department location. We found that this had not yet been completed, which contributed to the incomplete inventory. The OCIO told us it did not have a plan for enforcement.

Regular testing of wireless network security and monitoring for potential rogue wireless access points are recognized best practices that strengthen the Department's overall IT security posture. A breach of a Department wireless network has the potential to adversely affect operations and result in the loss of sensitive data.

[14] A rogue access point is an unauthorized access point that has been attached to a secured network. While sometimes installed with malicious intent, it is commonly installed by employees for ease of use. An evil twin attack is intended to masquerade as an authorized access point with malicious intent. While both are unauthorized, or "rogue," there are significant differences in the available methods to detect and respond to each.

Recommendations

We recommend that the OCIO:

9. Initiate an internal audit to identify and inventory all existing wireless networks Departmentwide. The inventory should include all ESN connected, Government-funded equipment not connected to ESN, and hotspots used in a group setting by multiple staff for performing daily duties (not single-user hotspots)

10. Disconnect and shut down all wireless networks that are not authorized or approved through the OCIO's new formal process

11. Require that all wireless operators implement a process to ensure that the Department's wireless network inventory is updated regularly to ensure completeness and accuracy

Contradictory, Outdated, and Incomplete Guidance

We found that wireless networks throughout the Department were not standardized because the guidance provided by the OCIO was contradictory, outdated, and incomplete. NIST requires agencies to (1) establish usage restrictions, configuration and connection requirements, and implementation guidance for wireless access, and (2) define a baseline configuration standard for all systems.[15]

The OCIO's *Security Technical Implementation Guide 802.11x Wireless Systems* (STIG) contained contradictory guidance, outdated material, incorrect definitions, and flawed risk priorities. For example:

- The document did not actually provide the baseline configuration as required by NIST.

- Some configuration options were listed as optional in one section but required in other sections of the STIG.

- The document was based on or refers to outdated material that, on average, was 12 years old. In many cases, links to reference material and guidance are no longer maintained.

- Technical terminology was frequently misused (e.g., "rogue access point" versus "evil twin").

- The STIG places more emphasis on attacks that occur after unauthorized access is obtained than it does on attacks that can be used to gain access in the first place.

[15] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Additionally, we found the guidance did not address the most common and modern attack vectors. Our testing shows that the Department's wireless networks are vulnerable to these significant and well-known wireless security attacks with easy-to-use exploits. Some of the attacks that should be addressed include:

- Evil twin exploit tools – first published in 2008
- WiFi Protected Setup (WPS) exploit tools – first published in 2011 and 2014
- Vulnerability resulting in easier pre-shared key collection – first published in 2018

The OCIO's wireless policy and requirements do not address how to configure networks that are not directly connected to the ESN. This includes facilities using wireless capability provided by a cable, DSL, or cellular internet service provider. Several of the bureaus and offices we visited operated wireless networks that were not secure on non-ESN connections, although many of these could not be validated due to the lack of inventory.

Some of the confusion stems from the fact that the STIG contains artifacts from previous revisions. According to the document changelog, the purpose of the document has changed several times over the past 9 years, resulting in a disjointed mixture of standards, policies, procedures, and configuration guidance.

Recommendations

We recommend that the OCIO:

12. Issue clear policy and procedures that address all types of wireless networking scenarios

13. Replace the *Security Technical Implementation Guide 802.11x Wireless Systems* document with an updated, actionable, and relevant STIG that clearly outlines, in detail, the minimum required controls for all departmental wireless networks, including existing networks

14. Review its Security Technical Implementation Guide periodically (annually at a minimum) for outdated or compromised configurations and update accordingly

Conclusion and Recommendations

Conclusion

The Department's failure to securely configure wireless networks has put its wireless and internal networks at high risk of compromise. Its poor cyber risk management practices significantly contributed to the security weaknesses we found. Moreover, the Department's lack of network segmentation greatly amplifies the potential adverse effect to the Department if an attacker gains unauthorized access to a bureau or office network. These issues occurred because the OCIO failed to adequately manage the Department's wireless program.

As part of our evaluation, we gained access to internal computer networks by exploiting wireless network vulnerabilities from publicly accessible areas in departmental facilities. We used well-known attack techniques including evil twin, which was first identified 15 years ago. After gaining access to internal networks, we scanned ranges of network addresses and identified high-value IT assets. A breach of a high-value IT asset would have a severe adverse effect on operations or result in the loss of sensitive data.

Effectively implementing security controls across such a diverse, decentralized, and interconnected infrastructure is a very difficult and complex goal. Any misconfiguration or inherent weakness in one technology can have a domino effect that allows an attacker to pivot from one system to the next, one bureau to the next, repeatedly. Without an adequate foundation of configuration guidance, technology requirements, and standard procedures, it is unlikely the Department will be able to reach a secure state with its wireless infrastructure.

Until the Department improves its cyber risk management practices, its computer networks and high-value IT assets will be at risk of compromise, the results of which could have serious or severe adverse effect on Department operations, assets, or individuals. The Department has begun taking significant steps to mitigate these weaknesses, but more remains to be done.

With over 2,200 facilities and an unknown number of wireless access points, the available options for attackers have increased significantly. We were able to visit only 91 of the Department's facilities, and time spent at each was very limited. Therefore, this report should not be considered a complete analysis of all wireless networking within the Department. Significant weaknesses may still be present and offering malicious actors an easy entry point. The Department must evaluate the increased risk insecure wireless networks pose to its information resources and prioritize identifying and securing its wireless infrastructure.

OCIO Response

In response to our draft report, the OCIO concurred with all 14 recommendations and stated that it is working to implement them. The OCIO is updating its governance of wireless networking through a suite of new and updated program documents including policy, architectural guidance, testing, and monitoring and enforcement by the bureaus. The OCIO and affected bureaus stated that the technical conditions that led to our findings have been resolved. Based on these responses, we consider 13 of the 14 recommendations resolved but not implemented.

We disagreed with the OCIO's proposed solution and statement that the technical issues have been resolved for Recommendation 3. We met with the OCIO to discuss ongoing concerns and additional steps that may be taken to more effectively secure the Department's infrastructure in the event a wireless network breach occurs. We clarified Recommendation 3 based on those discussions. The OCIO will perform additional risk analysis regarding network segmentation of its wireless networks and determine what additional steps may be required to satisfy this recommendation's goals. Until then, we consider this recommendation unresolved.

Recommendations Summary

We recommend that the OCIO:

1. Require and enforce the use of mutual certificate authentication (client and server) for all ESN connected networks, specifically prohibiting pre-shared key authentication for ESN connected networks

2. Require an additional layer of encryption not provided by the wireless network for any official use of non-ESN connected networks that use pre-shared key authentication, such as forced VPN connections

3. Implement network segmentation to isolate clients connected to bureau wireless networks from accessing unrequired resources at other bureaus

4. Perform periodic audits and penetration testing of wireless networks, regardless of security categorization

5. Establish a standard operating procedure that defines indicators of malicious wireless activity and defines when and how to perform and record investigations of those activities

6. Establish an SOP to treat evil twin alerts as a high-level threat

7. Establish an SOP to implement a wireless intrusion prevention system to suppress suspected evil twin attacks

8. Include wireless infrastructure when developing dedicated group of incident responders to perform threat hunting and containment activities (building on Recommendation 11 from Report No. 2016-ITA-020)

9. Initiate an internal audit to identify and inventory all existing wireless networks Departmentwide. The inventory should include all ESN connected, Government-funded equipment not connected to ESN, and hotspots used in a group setting by multiple staff for performing daily duties (not single-user hotspots)

10. Disconnect and shut down all wireless networks that are not authorized or approved through the OCIO’s new formal process

11. Require that all wireless operators implement a process to ensure that the Department’s wireless network inventory is updated regularly to ensure completeness and accuracy

12. Issue clear policy and procedures that address all types of wireless networking scenarios

13. Replace the Security Technical Implementation Guide 802.11x Wireless Systems document with an updated, actionable, and relevant STIG that clearly outlines, in detail, the minimum required controls for all departmental wireless networks, including existing networks

14. Review its Security Technical Implementation Guide periodically (annually at a minimum) for outdated or compromised configurations and update accordingly

Appendix 1: Scope and Methodology

Scope

The scope of this evaluation includes wireless networks throughout the U.S. Department of the Interior. We conducted our technical testing between June 18, 2018, and June 30, 2019.

Methodology

To accomplish our evaluation objectives, we conducted data calls to the Department and bureaus and reviewed:

- Inventories of wireless and wired networks
- Policies and procedures
- Technical implementation and configuration documentation

Because the wireless inventory provided by the Department was incomplete, we selected the locations for technical testing from the wired inventory centered on four major metropolitan areas.

We further narrowed the selection based on:

- Inclusion in the wireless inventory provided by the Department
- Driving time from the local airport
- Size of the facility
- Wireless data available from public sources (e.g., Wigle.net)
- Accessibility (e.g., attempt to determine whether the facility had publicly accessible areas)

To accomplish our technical testing objectives, we:

- Developed custom hardware platform for conducting wireless testing
- Developed reconnaissance testing procedures for:
    - Collecting information about wireless networks at each site visited

    - Determining whether observed wireless networks were likely to belong to the bureau or office at that location, if not included in the wireless inventory (based on descriptive network names, strong signals inside facilities, etc.)
    - Manually reviewing collected wireless network data
    - Customizing scripts for automated review of collected wireless network data

- Developed technical testing procedures for:
    - Collecting credentials from pre-shared key networks
    - Collecting credentials from enterprise user authenticated networks using evil twin attacks[16]
    - Decrypting wireless traffic
- Developed post-exploitation testing of the Department's internal networks, including:
    - Custom scripts to perform internal network scans to identify whether:
        - The wireless network was isolated from internal networks
        - High-value IT asset networks were accessible
    - Manual testing of captured credentials against internal systems

We conducted our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

[16] Disclaimer: When a client successfully connects to an evil twin, the attacker can forward client traffic to other networks (such as the internet) and eavesdrop on that client's communications. Our testing focused only on acquiring the encoded credentials when clients connected to our units. We did not provide network access to clients after they connected to our evil twin.

Appendix 2: Response to Draft Report

The OCIO provided an appendix with detailed information on how it plans to address our findings and recommendations. Due to the sensitive nature of the content, and in agreement with the OCIO, the additional details provided in the appendix have been removed from the public version of this report. The Department's response to our draft report follows on page 25.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

August 14, 2020

Memorandum

To: Mark Lee Greenblatt
Inspector General

From: William E. Vajda
Chief Information Officer

WILLIAM VAJDA

Digitally signed by WILLIAM VAJDA
Date: 2020.08.14 18:27:45 -04'00'

Subject: Office of the Chief Information Officer (OCIO) Response to Draft Evaluation Report – *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks,* Report No. 2018-ITA-020

Please find attached the Office of the Chief Information Officer (OCIO) Management Response. We listed all attachments below for your reference and review.

I am pleased to report that the Department not only concurs with all of the Office of the Inspector General's (OIG) recommendations, but also we have already substantially complied with all of them, with just a few remaining tasks to be accomplished with respect to a few of the recommendations. We appreciated working with you and your office on these recommendations.

If you have questions, please contact me at (202) 208-6194. If your team members have any questions, please direct them to Richard Westmark, Chief, Compliance and Audit Management (CAM) [redacted]@ios.doi.gov).

Attachments:

1. OCIO Management Response to OIG Report No. 2018-ITA-020 Recommendations
2. Appendix A

cc: John (Jack) Donnelly, DOI Chief Information Security Officer, OCIO
Richard Westmark, Chief, Compliance and Audit Management Branch, OCIO
Dr. Chadrick Minnifield, Chief, Internal Control and Audit Follow-up, Office of Financial Management

Management Response to OIG Report No. 2018-ITA-020 Recommendations

Introduction and Overview

The U.S Department of the Interior (DOI) Office of the Chief Information Officer (OCIO), in coordination with the bureau and office Associate Chief Information Officers (ACIOs), prepared the management response for the *Evil Twins, Eavesdropping, and Password Cracking: How the Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Network*, Report No. 2018-ITA-020.

The OIG initiated the Notice of Evaluation in January 2018, ultimately resulting in the attached recommendations. The OIG noted that they found the BisonWiFi and BisonGuest wireless networks were operationally sound and secure. As a result, the OIG offered no significant findings for the Department-wide wireless infrastructure. The OIG concluded that the BisonWiFi evaluation results demonstrated good design, implementation, and operational monitoring services. BisonWiFi implements standard wireless network configurations recommended as best practices by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-97 *Establishing Wireless Robust Security Networks* and NIST SP 800-153 *Guidelines for Securing Wireless Local Area Networks.*

Starting in 2019, the OCIO enforced the implementation of the OIG's recommended security solution across all bureaus and offices accessing the DOI networks. The DOI concurrently issued management guidance that came into effect in FY2020 that requires annual assurance statements from the DOI bureaus and offices to confirm they are in compliance with all statutory, regulatory, and OCIO policy directives governing the use of information technology (IT) within their operations. Departmental policy requires bureaus and offices that operate wireless networks to complete a wireless inventory, auditing, and penetration testing on an annual basis, as required by the OCIO Architectural Security Guidance. The OCIO provides a web portal with information on how to configure and use a secure wireless service, as well as, instruction on maintaining a directory of bureau and office wireless networks and inventories. The OIG's specific recommendations and the OCIO's responses regarding these matters are attached. As noted previously, we have already substantially complied with all of the recommendations.

Through the Annual Assurance Statement process, bureaus and offices report and confirm their compliance, based upon self-assessment results of their wireless networks internal controls assessments and audits conducted on their wireless networks.

OIG RECOMMENDATION 1: Require and enforce the use of mutual certificate authentication (client and server) for all ESN connected networks, specifically prohibiting pre-shared key authentication for ESN connected networks.

Management concurs with recommendation 1 and has substantially completed efforts to comply with this recommendation. Specifically, since March 2018, the *DOI Security Technical Implementation Guide (STIG) 802.11x Wireless Systems* (a document that provides detailed procedures for securing DOI's Wireless Systems) prohibited using "Pre-shared Keys" to connect to the enterprise network. Beginning in FY 2020, the STIG required all enterprise connected wireless networks to implement Extensible Authentication Protocol – Transport Layer Security (EAP-TLS), i.e. mutual certificate authentication method, requiring Personal Identity Verification (PIV). While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 2: Require an additional layer of encryption not provided by the wireless network for any official use of non-ESN connected networks that use pre-shared key authentication, such as forced VPN connections.

Management concurs with recommendation 2 and has substantially completed efforts to comply with this recommendation. Prior to the evaluation, users were required to connect to Department enterprise resources via a virtual private network (VPN) or application encrypted connectivity. Since March 2018, the STIG prohibited using "Pre-shared Keys" to connect to the enterprise network. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 3: Implement network segmentation for the Department and all bureaus, at the very least for wireless networks

Management concurs with recommendation 3 and has substantially completed efforts to comply with this recommendation. Since late 2019, the STIG has required a level of segmentation for enterprise connected wireless networks. Non-enterprise connected wireless networks were already segmented by design. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official: John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date: November 1, 2020

[redacted]

OIG RECOMMENDATION 4: Perform periodic audits and penetration testing of wireless networks, regardless of security categorization

Management concurs with recommendation and has substantially completed efforts to comply with this recommendation 4. The Department updated the STIG to require these recommended activities for all operators of enterprise connected wireless networks. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official: John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date: November 1, 2020

[redacted]

OIG RECOMMENDATION 5: Establish a standard operating procedure that defines indicators of malicious wireless activity and defines when and how to perform and record investigations of those activities

Management concurs with recommendation 5 and has substantially completed efforts to comply with this recommendation. The Department updated the STIG to enhance standard operating procedures to address indicators of malicious wireless activity and associated reporting to incorporate lessons learned from this evaluation's findings. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official: John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date: November 1, 2020

[redacted]

OIG RECOMMENDATION 6: Establish an SOP to treat evil twin alerts as a high-level threat

OIG RECOMMENDATION 7: Establish an SOP to implement a wireless intrusion prevention system to suppress suspected evil twins

Management concurs with recommendations 6 and 7 and has substantially completed efforts to comply with these recommendations. The Department updated the STIG to enhance standard operating procedures with respect to evil twins to incorporate lessons learned from this evaluation's findings. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 8: Include wireless infrastructure when developing dedicated group of incident responders to perform threat hunting and containment activities (building on Recommendation 11 from Report No. 2016-ITA-020)

Management concurs with recommendation 8 and has substantially completed efforts to comply with this recommendation. The Department updated the STIG to require the recommended activities, leveraging existing technology and incident responders, for all operators of enterprise connected wireless networks. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 9: Initiate an internal audit to identify and inventory all existing wireless networks Department-wide. The inventory should include all ESN connected, Government-funded equipment not connected to ESN, and hotspots used in a group setting by multiple staff for performing daily

Management concurs with recommendation 9. Hotspots (e.g. government phones with wireless network hotspot capabilities) are maintained through another inventory control process (Mass360 prior to this report evaluation). Since late FY 2019, the Department has maintained a wireless network inventory and geolocates enterprise connected wireless networks on the Information Management and Technology Leadership Team (IMTLT) Services site for traveling customers. The baseline inventory was completed in late FY 2019. Geolocation mapping occurred in early FY 2020. While these interim measures are in place, actions are necessary to update the wireless inventory. As such, the following actions need to be taken to close the recommendation: (1) starting in FY 2020, bureaus and offices will submit updated wireless inventory via their annual assurance statements; (2) Departmental release of wireless inventory updates; and (3) submission of closure request to the OIG.

Responsible Official:	Deborah (June) Hartley, Deputy CIO for Bureau Office Support
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 10: Disconnect and shut down all wireless networks that are not authorized or approved through the OCIO's new formal process

Management concurs with recommendation 10 and has substantially completed efforts to comply with this recommendation. The Department will continue to use its delegate approval and authorization processes in accordance with policy. The Department disconnected or shutdown STIG non-compliant wireless networks and will continue to do so through formal process. Further, enterprise connected wireless networks cited in this report were timely disconnected or isolated, then remediated to ensure STIG compliant EAP-TLS and PIV implementation before reauthorizing operations. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 11: Require that all wireless operators implement a process to ensure that the Department's wireless network inventory is updated regularly to ensure completeness and accuracy

Management concurs with recommendation 11 and has substantially completed efforts to comply with this recommendation. Specifically, since late FY 2019, the Department has maintained a wireless network inventory and geolocates enterprise connected wireless networks on the IMTLT Services site for traveling customers. The baseline inventory was completed late FY 2019. Geolocation mapping occurred in early FY 2020. While these interim measures are in place, actions are necessary to update the wireless inventory. As such, the following actions need to be taken to close the recommendation: (1) starting in FY 2020, bureaus and offices s will submit updated wireless inventory via their annual assurance statements; (2) Departmental release of wireless inventory updates; and (3) submission of closure request to the OIG.

Responsible Official:	Deborah (June) Hartley, Deputy CIO for Bureau Office Support
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 12: Issue clear policy and procedures that address all types of wireless networking scenarios

Management concurs with recommendation 12 and has substantially completed efforts to comply with this recommendation. The Department updated the STIG to explicitly include policy and procedures for wireless network scenarios or use cases. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 13: Replace the Security Technical Implementation Guide 802.11x Wireless Systems document with an updated, actionable, and relevant STIG that clearly outlines, in detail, the minimum required controls for all departmental wireless networks, including existing networks

Management concurs with recommendation 13 and has substantially completed efforts to comply with this recommendation. The Department updated the STIG to include minimum required security controls. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

OIG RECOMMENDATION 14: Review its STIG periodically (annually at a minimum) for outdated or compromised configurations and update accordingly

Management concurs with recommendation 14 and has substantially completed efforts to comply with this recommendation. The Department updated the STIG in 2018, 2019 and the latest updates reflect this report's recommendations. While these interim measures are in place, actions are necessary to make the STIG changes permanent. As such, the following actions need to be taken to close the recommendation: (1) bureau and office review and clearance of the STIG; (2) Departmental release of the approved STIG; and (3) submission of closure request to the OIG. The Departments is committed to periodic review of the STIG, at least annually.

Responsible Official:	John (Jack) Donnelly, Chief Information Security Officer
Target Completion Date:	November 1, 2020

[redacted]

Appendix 3: Status of Recommendations

Recommendations	Status	Action Required
1 – 2, 4 – 14	Resolved but not implemented	We will refer these recommendations to the Assistant Secretary for Policy, Management and Budget to track their implementation.
3	Unresolved	We will refer this recommendation to the Assistant Secretary for Policy, Management and Budget for resolution.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet:	www.doioig.gov	
By Phone:	24-Hour Toll Free:	800-424-5081
	Washington Metro Area:	202-208-5300
By Fax:	703-487-5402	

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240