



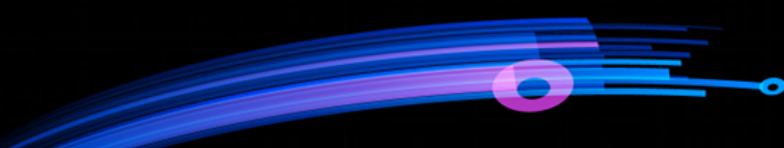
GUARDING INTELLECTUAL PROPERTY AGAINST CYBER ESPIONAGE



Ji-Yong David Chung
Kenneth M. Lesch
John Voisinet
Snyder Clark Lesch & Chung LLP
January 2016

In *Aeneid*, Virgil tells a story of the Trojan War. In the War, the battle-weary Greeks devised a plan to deceive the Trojans and take the city of Troy. Based on the plan, they built a large, hollow wooden structure now known as “the Trojan horse.” The Greeks hid elite soldiers inside the horse and left it near the impenetrable walls of Troy. The Greeks then concealed their army, to appear as if they had given up their siege and left to return to their homelands. Believing that their enemy had departed, the Trojans brought the horse within the city as a trophy. During the night, the elite soldiers crept out of the Trojan horse and opened the gates of Troy. The Greek army stormed into Troy through the open gates and destroyed the city.

Published online at
IP Law 360 (LexisNexis)
January 2016



I. Introduction

As reported in *The New York Times* in March of 2015, patent applications stored at law firms are targets of economic cyber espionage.¹ Since patent applications include sensitive client data, the report raises concerns about maintaining the confidentiality of information entrusted to law firms.

We address such concerns in this article. In particular, we examine Trojan Horse-like malware (“Trojan malware”) as the most common means for perpetrating cyber espionage, and present a simple and inexpensive solution that a client can request outside counsel to implement to protect patent related data (e.g., invention disclosure, unpublished patent application, etc.).

II. Trojan Malware Threat

To steal information, Trojan malware takes advantage of typical Internet-based communications. In figure 1, we illustrate Trojan malware in its network environment. As shown, the environment includes a *client*, a patent law firm (“*firm*”) and a *compromised site*. We do not show various network entities with which the client and the firm interact (e.g., the U.S. Patent and Trademark Office (USPTO), content providers, third party patent databases, cloud services, other clients, etc.).

In figure 1, the client sends a *document* that pertains to patent matters, such as an invention disclosure, to the firm. The document may pass through a network service used by the client (e.g., a patent-document management service, an email service, etc.). The firm

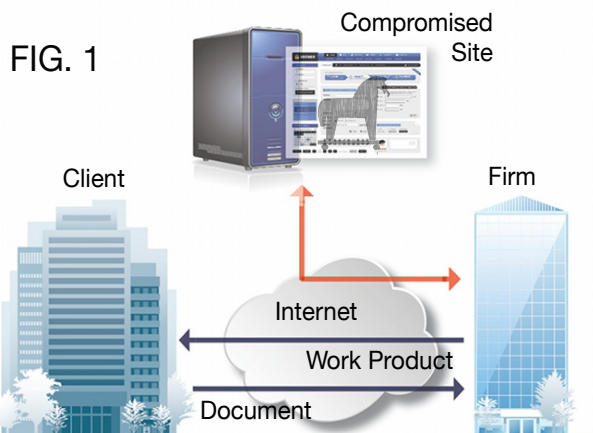
receives and stores the document, generates and stores *work product*, such as a draft patent application, and forwards the generated work product to the client, possibly through the same network service that the client used to forward the document.

The compromised site is infected with the Trojan malware, which has been planted by a cyber spy (e.g., a foreign government, a dishonest competitor, or a malicious group).

To access the document and work product stored at the firm, the cyber spy has to penetrate into the firm’s network. Just as Troy was protected by its impenetrable walls, however, the firm’s internal network is well guarded with its own digital walls (e.g., a firewall) against unsolicited network packets from outside the firm. Like the Greeks who deceived the Trojans, the cyber spy attempts to deceive someone at the firm and slip the Trojan malware into the internal network of the firm.

Because of the deception, Trojan malware intrusions are difficult to eliminate. In a typical workplace, employees need to access the Internet to obtain information required to perform tasks or to carry out online business transactions. Over an extended period, eventually someone at the firm will inevitably visit a site harboring Trojan malware, open a malicious document or otherwise unwittingly bring the malware into the firm.

Bringing the malware into the firm can lead to unauthorized disclosure of client information. As the firm attorneys, agents, and staff members interact with various online entities using multiple communication



devices, the firm accepts and *intermixes* vast quantities of foreign data. Therefore, if the Trojan malware is injected into an unguarded computer in the firm, the malware has ample opportunities to contaminate the data, infect interconnected computers, and gain control of the computers. In particular, the malware may capture and exfiltrate information entrusted to the firm.



In late 2013, attackers used a Trojan Horse virus to steal credentials for accessing Target's system, from one of its vendors. Using the credentials, the attackers infiltrated Target's network and installed malware on point-of-sales devices. The malware took 70 million customers' private information. The CEO and CIO lost their jobs, as credit card replacement and refunding costs rocketed to \$200 million. Then there were legal costs (over 140 lawsuits) and loss in profits (46% drop in the 4th quarter of 2013).²

III. Basic System Architecture

In view of the intermixing of foreign data, to guard against Trojan malware, the firm can implement a system that isolates sensitive client documents and work product from other information. Figure 2 illustrates one such system. The system architecture is based on the concepts that a famous security expert, Bruce Schneier, describes in his blog post, "Air Gaps."³ The system is simple and inexpensive for any firm to implement at the request of a client.

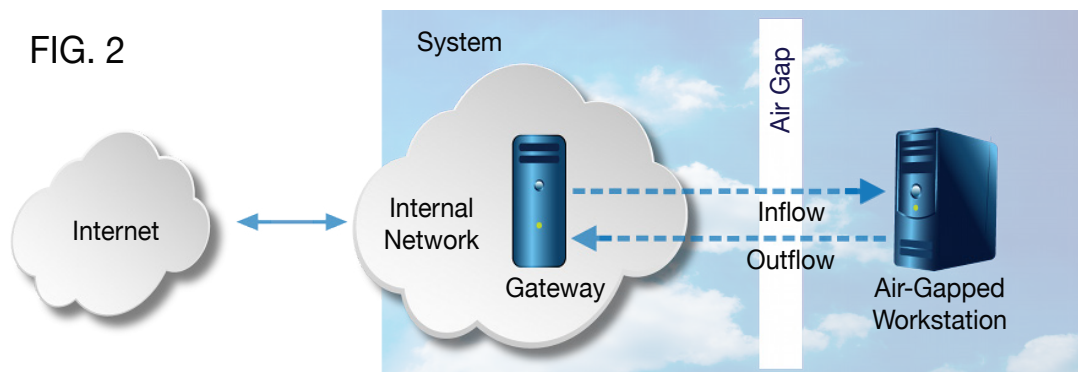
As shown, the system includes a *gateway* and an *air-gapped workstation*. The gateway is a stripped-down computer (e.g., specially configured with minimum software and hardware) whose only functions are to receive sensitive documents from the client, send work product to the client, and communicate with the USPTO over the Internet.

The air-gapped workstation is a stripped-down computer that is isolated from the Internet. The main function of the air-gapped workstation is to provide a secure, isolated platform for storing client information and for generating the work product.

To ensure the isolation, the air-gapped workstation is communicatively decoupled not only from the Internet, but also from the firm's internal network by a physical barrier. In figure 2, the physical barrier is the *air gap*. When client information is stored at the workstation, the air gap shields it against hidden malware that may have been brought into the internal network of the firm.

To use the workstation, after a sensitive client document has been downloaded from the client onto the

FIG. 2

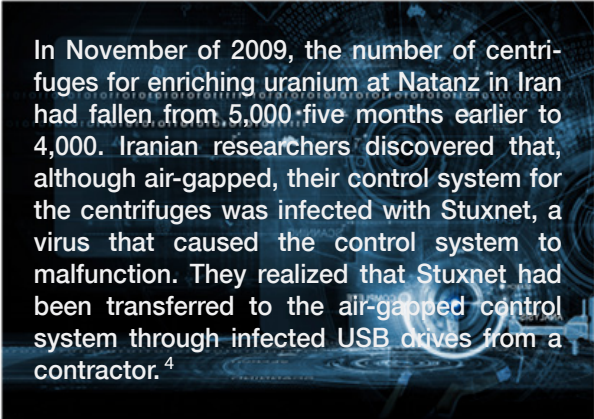


gateway, it is securely transferred from the gateway to the workstation across the air gap. The copy of the document on the gateway is then securely erased (e.g., overwritten).

At the workstation, a member of the firm generates the work product based on the client document. When complete, the work product is securely transferred from the workstation to the gateway across the air gap, and then transmitted from the gateway to the client. The copy of the work product on the gateway is then securely erased.

This *inflow* and *outflow* of information to and from the workstation requires the use of portable storage media. For example, for the inflow, a member of the firm copies the document from the gateway to a write-once compact disk (CD), physically carries the CD from the gateway to the workstation across the air gap, and copies the document on the CD to the workstation. For the outflow, a member of the firm performs actions similar to those performed during the inflow, but for transferring the work product from the workstation to the gateway.

Special care must be taken when using portable storage media for the inflow and outflow. If a portable storage medium has been exposed to devices other than the gateway and the workstation, for example, it could also have been exposed to malware and should not be used to transfer information for the inflow and outflow. Preferably, the portable storage medium stores contents in an encrypted form, in case the medium is lost. A storage device not specifically determined as secure should not be used to convey information between the gateway and the workstation.



In November of 2009, the number of centrifuges for enriching uranium at Natanz in Iran had fallen from 5,000 five months earlier to 4,000. Iranian researchers discovered that, although air-gapped, their control system for the centrifuges was infected with Stuxnet, a virus that caused the control system to malfunction. They realized that Stuxnet had been transferred to the air-gapped control system through infected USB drives from a contractor.⁴

Common burdens associated the inflow and outflow can be greatly reduced when the system is used only for the most sensitive documents (e.g., invention disclosures and draft applications).

IV. The Gateway

When the firm intermixes foreign data, which includes both client documents and data from a large number of sites, the firm exposes the client documents to potential sources of infection and data-stealing malware. The use of the air-gapped workstation resolves this problem by isolating the client information and work product from other data. This measure, however, does not address the issue of firm members inadvertently visiting a malicious site on computers connected to the Internet and bringing malware into the firm.

We address this issue by specially configuring the gateway and network elements on which the gateway relies for communication (e.g., a firewall, router in the firm's internal network, email program and server in the Internet, etc.). The configuration restricts the gateway to communicate only with selected devices and sites (e.g., name servers, the client, the USPTO, a patent-document management service, etc.). This reduces the probability of a browser on the gateway visiting a malicious site or the probability of an email program receiving an ill-intentioned email message.

When the gateway is thus restricted, a user's actions at the gateway are constrained, which reduces the amount of foreign data downloaded to the gateway and lessens the exposure of client information to the foreign data. The concept goes hand-in-hand with the idea that, as described above, the gateway stores the client document only temporarily, until the document is conveyed to the workstation and erased from the gateway. The erasure of the document from the gateway shortens the time during which the document is exposed to the foreign data.

V. End-to-End Encryption

Generally, as long as a firm communicates over the Internet, the risk of malware infiltrating a firm computer cannot be entirely eliminated. To defend against this risk, however, the client can encrypt its documents prior to sending them to the firm. The firm keeps the documents encrypted until the documents

are safely conveyed to the air-gapped workstation. Only then are the documents decrypted. The purpose of this end-to-end encryption (i.e., from the client to the workstation) is to reveal the contents of the sensitive client document to a user only when it is most isolated in the firm (i.e., in the air-gapped workstation).

Likewise, the work product is encrypted at the workstation before the work product is transferred to the gateway. The firm keeps the work product in the encrypted form as it is delivered from the workstation to the client through the gateway.

Many clients rely solely on Transport Layer Security (TLS)/Secure Socket Layer (SSL)-based communications (e.g., HTTPS) to exchange information with the firm. Although TLS/SSL affords significant protection, TLS/SSL-based communications cannot render a full end-to-end encryption of the document and the work product across the air gap.

VI. Per-Client Isolation

Some patent law firms use a single document management system to protect documents that belong to different clients. As a result, all of the documents become available to a cyber spy when the spy breaks into the document management system. All of the client documents are under the same security risk regardless of client or sensitivity.

Because different clients attract different levels of attacker interests, however, a particular client may not want its documents to face the same security risk as documents that belong to other clients. In such a situation, the client should request the firm to allocate a separate gateway and a separate air-gapped workstation. This affords per-client isolation of its documents and work product from information that belongs to other clients. Per-client isolation prevents malware at a document of one client from spreading to those of other clients.

VII. Conclusions

Seven hundred years after the Trojan War, Histiaeus, a former tyrant of Miletus (a city in Greece), contrived to push his son-in-law Aristagoras to lead an insurrection against the Persians. To this end, Histiaeus shaved the head of his most trusted slave and tattooed a message on the slave's head. When the

slave's hair grew back, Histiaeus dispatched him to Aristagoras. Aristagoras then re-shaved the slave's head to read Histiaeus's message.⁵

Histiaeus went to great lengths to safeguard his message, for he could have lost his head had his plan been discovered by Persian spies. With current technologies, we have much easier ways to protect our client's data from spies. One solution is the system discussed in this article. The system is simple and inexpensive for patent law firms to implement, and allows the firms to allocate more resources to provide improved services to clients.



¹ Matthew Goldstein, "Citigroup Report Chides Law Firms for Silence on Hackings," *The New York Times*, 26 Mar. 2015, <http://www.nytimes.com/2015/03/27/business/dealbook/citigroup-report-chides-law-firms-for-silence-on-hackings.html>, Web. 3 Dec. 2015.

² Teri Radichel, "Case Study: Critical Controls that Could have Prevented Target Breach," *SANS Institute InfoSec Reading Room*, 5 Aug. 2014, pp. 2-4, <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412>, Web. 3 Dec. 2015.

³ Bruce Schneier, "Air Gaps," *Schneier on Security*, 11 Oct. 2013, https://www.schneier.com/blog/archives/2013/10/air_gaps.html, Web. 28 Nov. 2015.

⁴ Kim Zetter, "AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON," *Wired*, 3 Sep. 2014, <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet>, Web. 3 Dec. 2015.

⁵ Richard, J, *Histiaeus, d.c. 494/493*, http://www.historyof-war.org/articles/people_histiaeus.html, Web. 4 Dec. 2015.



About the Authors

JiYong David Chung is one of the founding partners at Snyder Clark Lesch and Chung, LLP, a boutique Intellectual Property law firm. David received his BSEE from Massachusetts Institute of Technology, MSEE from the University of Rochester, and JD from George Washington University. David served as a Computer Scientist at Stanford Telecommunications, Inc. for two years and at the United States Patent and Trademark Office for six years prior to practicing patent law.

Kenneth M. Lesch is a patent attorney who used air-gapped networks while previously working as an electrical engineer in the defense industry. Ken has also drafted patent applications on an air-gapped workstation and used dedicated single-purpose communication gateways as described in this article. Ken practices patent law at Snyder, Clark, Lesch & Chung, LLP and specializes in communication networks, signal processing, and analog circuits.

John Voisinet prepares and prosecutes patent applications at Snyder, Clark, Lesch and Chung, LLP. John received his BSEE from University of Michigan-Dearborn and JD from George Mason University. John was an Examiner at the USPTO, examining applications directed to video technology. Prior to entering the patent field, he worked as an electrical engineer performing systems engineering and digital signal processing algorithm design in the defense and automotive industries.
