



Owl Products Help Manage Medical Information Security in Compliance with HIPAA Regulations

Abstract:

Owl Computing Technologies offers a secure one-way data transfer system that provides significant security benefits for IT architectures that transfer large volumes of medical information in electronic form. Owl systems satisfy numerous security specifications in a cost effective way, and are most useful for data processing scenarios where data can be “pushed” from the sending side of a network connection. When considering return on investments (ROI) for IT equipment purchases, it is useful to consider the value of a network security system by comparing the cost of its installation with the legal cost of defending its absence when security is compromised.

Author: Jeffrey Menoher

Owl Computing Technologies, Inc.
38A Grove Street, Suite 101
Ridgefield CT 06877
<http://www.owlcti.com>
Ph: 203-894-9342
Fax: 203-894-1297

Document ID: productAppMedicalInfo_05e
Document Release: 05e
Publish Date: 6/21/2006

Table of Contents

| | |
|--|----|
| Owl Products Help Manage Medical Information Security in Compliance with HIPAA Regulations | 1 |
| 1 Introduction..... | 3 |
| 2 Owl One-Way Data Transfer Systems..... | 4 |
| 2.1 Owl’s Core Product, the One-Way Link..... | 4 |
| 2.2 Data Transmission at Transport Layer..... | 5 |
| 2.3 General Applications | 6 |
| 3 Federal Regulations: | 7 |
| 3.1 Administrative safeguards | 8 |
| 3.1.1 Risk analysis | 8 |
| 3.1.2 Risk Management | 9 |
| 3.2 Physical safeguards..... | 9 |
| 3.3 Technical safeguards..... | 9 |
| 4 System Configuration Scenarios using Owl Products | 10 |
| 5 Owl Systems in Context of Overall Network Security..... | 13 |
| 6 Conclusion | 13 |
| 7 References..... | 14 |
| 8 Revision History | 15 |

Table of Figures

| | |
|---|----|
| Figure 1: Send/receive pair of network interface cards, Version 4 cards shown..... | 4 |
| Figure 2: Secure one-way link between networks. Blue sends, Red receives. | 5 |
| Figure 3: Remote users send medical data to central secure repository | 11 |
| Figure 4: Data transfer of zipped, encrypted files from one secure network to another... .. | 12 |
| Figure 5: Secure medical data transfer to read-only access area | 12 |
| Figure 6: Controlled distribution of medical information from secure repository | 12 |
| Figure 7: secure printing from protected network | 13 |

1 Introduction

The nature of modern telecommunications has changed the nature of medical treatment. A physical examination may occur at one location, and the resulting data may be electronically transferred to a distant geographical location for examination by a specialist. Medical billing involves multi-party payment arrangements that are increasingly automated and involve electronic transfer of medical information to more locations.

Health care service providers outsource many of their IT functions to medical information “clearing houses”; specialized IT firms with expertise in the field. Clearing house data may include actuarial data for health care providers and government agencies. Some government agencies, like the Center for Disease Control (CDC), collect medical information in real-time and on a large scale.

While medical information is more widely distributed than ever before, it is also private and sensitive, and the consequences for its mishandling are costly.

The management of medical information is regulated by the federal government, which has set standards for its storage, access, and transport in electronic form. Federal regulations pertaining to management of medical information are based on requirements first defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and clarified under the Code of Federal Regulations (CFR). New federal regulations are forcing rapid deployment of Information Technology (IT) security measures in the medical community that were previously used by government intelligence services and large financial organizations.

Significant hardening of existing networks are achieved by separating inter-network communications into one-way data transfers. One-way data transfers naturally compliment the inherently different security checks required for transferring data to (read-up) or from (read-down) any isolated high-security domain. Among other advantages, one-way data transfers deny the possibility of network probing for vulnerability; a prelude for most cyber-attacks. Intelligent utilization of one-way data transfer also simplifies creation of data archives whose contents cannot be deleted, corrupted, or repudiated.

Owl Computing Technologies offers a secure one-way data transfer system that provides significant security benefits for IT architectures that handle medical information in electronic form. Owl systems satisfy numerous stringent security specifications in a cost effective way, and are most useful for data processing scenarios where large volumes of data can be “pushed” from the sending side of a network connection.

This paper describes Owl systems, and their suggested deployment in various medical settings that are subject to federal regulations regarding information security.

2 Owl One-Way Data Transfer Systems

Owl products are one-way data transfer systems that provide security in both the physical and logical sense. They are used to isolate high security networks from external threats, while allowing them to import or export data at high speed in a controlled way.

Unlike commercially available firewalls, Owl hardware is designed to pass information in one direction only at high throughput rates (155 Mbps OC-3). In the reverse direction, it is physically impossible to send messages of any kind. Owl systems cannot be hacked with software, and are widely used by US government intelligence agencies for isolating their high security networks.

All Owl hardware is EAL certified, according to Common Criteria standards jointly developed by the National Institute of Standards (NIST), the National Security Agency (NSA), and a small number of similar organizations in the U.K., Canada, France, Germany, and the Netherlands. Using non-specialized “commodity” components from the telecommunications industry, our latest generation (version 3) Owl hardware attained the widely respected EAL4 certification by subjecting its engineering designs to rigorous independent security analysis. Prototype version 4 cards, shown below in Figure 1, are in process of certification at higher levels. Owl continues to actively develop and improve its products in performance, function, and certifications.

2.1 Owl’s Core Product, the One-Way Link

Owl’s core product comprises two physically modified Asynchronous Transfer Mode (ATM) network interface cards and an optical fiber as shown in Figure 1. The two network cards fit into standard 32 bit PCI slots in their respective (separate) host machines, and they communicate through the optical fiber. The Send card LED output power is rated for optical fibers up to 2 km in length.

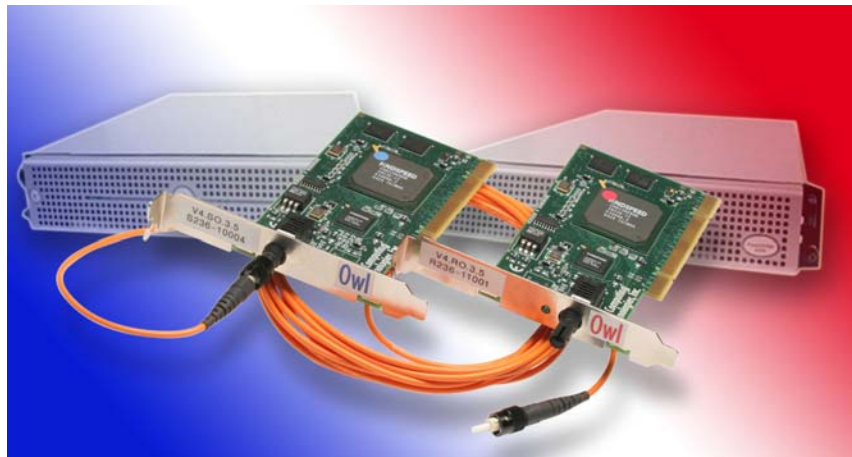


Figure 1: Send/receive pair of network interface cards, Version 4 cards shown.

All components are color-coded: Blue for Send, and Red for Receive. The Send card resides in the source computer (Blue), and is populated only with components for phototransmission. The Receive card resides in the destination computer (Red), and is populated only with components for photodetection. One-way data transmission is thus enforced at both ends of the fiberoptic cable creating a “Dual Diode” data transfer system; a truly secure one-way link between networks as shown in Figure 2.

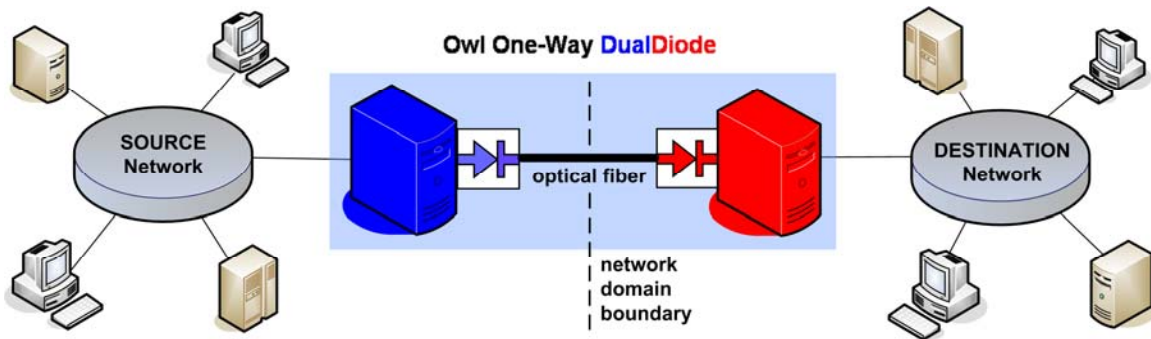


Figure 2: Secure one-way link between networks. Blue sends, Red receives.

With Send and Receive cards installed, the host platforms become the data transmission gateways for their respective networks as shown above. Source data may originate from any network location accessible to the Blue machine, which sends it to the Red machine through the Dual Diode. Once in the Red machine, data may be forwarded to any destination location accessible to the Red machine. Data types include files, directory structures, TCP packets, and UDP datagrams. High data throughput supports multiple users for each hardware installation.

The One-Way Transfer is a dedicated Point-to-Point optical link and is not a connection-oriented communication scheme. No mitigating firewall is required between the send and receive nodes. However, the Owl system does not perform content filtering or encryption, and the user may elect to install a firewall or additional security features on the network.

Customer equipment may be connected to any type of network that may be in use. Network types include Ethernet, Token-Ring, and FDDI.

2.2 Data Transmission at Transport Layer

The actual data transfer is performed through a patented protocol that does not involve the TCP/IP stack, and does not pass IP information across the link. IP routes are defined at the time of system configuration in the form of channel mapping tables, which will be described in greater detail below.

When IP packets are received by the Send (Blue) computer, IP information normally carried in the packets is replaced with pre-assigned channel numbers. After passing across the one way link, the channel numbers are mapped to their predetermined IP destinations in the Receive (Red) computer. The mapping tables residing in Send and Receive machines are different. Neither table alone can be used to construct the other, and neither table alone provides IP routing information that might compromise security of the overall system.

Since no message traffic is possible from Receiver to Sender, the one way link proxies, but cannot fully implement two-way protocols, such as TCP/IP. This fact carries several significant implications related to data verification and relative machine performance requirements which are described below.

Data integrity is verified in several ways during transfer across the one-way link. At the ATM cell level, data integrity is verified in hardware according to the AAL5 communication protocol. Advanced hash algorithms are used to verify the integrity of data at the IP packet level. The Send machine calculates a hash number for the contents of each packet, the Receive machine recalculates the hash number, and the results are compared. In the rare occurrence of unequal hash numbers, the packet is dropped and an error is logged. Packet sequence numbers are tracked. The integrity of larger data structures assembled from IP packets is verified in similar fashion.

Owl systems have proven exceptionally reliable. They are built by American manufacturers adhering to rigorous quality control standards and subject to multiple-day burn-in tests prior to shipment. When Send and Receive machines are matched in performance and properly configured, packet losses are extremely rare. Owl systems reliably transfer large files with sizes exceeding 1 terabyte. Since 1998, no Owl system has failed in the field.

2.3 General Applications

Owl systems are most useful for high-throughput data processing scenarios where data can be “pushed” from the sending side of a network connection. General scenarios include

1. Accumulation of medical data in a secure centralized repository
2. Replication of medical data from one secure repository to another
3. Copying protected data from a secure repository to a read-only security area for controlled access
4. Direct dissemination of medical data from a secure centralized repository, including secure printing

Application scenarios for medical information will be described in greater detail below.

3 Federal Regulations:

Government documents state:

“...The Department of Health and Human Services (HHS) Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information...”

Federal regulations pertaining to management of medical information are based on requirements first defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and clarified under the Code of Federal Regulations (CFR), Title 45, Volume 1, Subtitle A, part 164 “Security and Privacy”. This information can be accessed at website: http://www.access.gpo.gov/nara/cfr/waisidx_04/45cfr164_04.html

Three sections of Part 164 pertain to storage, access, and transport of medical information in electronic form, and are of particular interest for the purposes of deploying Owl products.

164.308 Administrative safeguards

164.310 Physical safeguards

164.312 Technical safeguards

These sections describe electronic data accessible through computer workstations and the physical environment in which people and computers operate.

Other sections specify which users and organizations have legal rights of access to medical information, under what contractual terms, and how the data is to be managed.

Note that the requirements described in various sections are complimentary. Safeguards intended for electronic data access may be reconfigured by a negligent or malicious person who gains physical access to a secure facility. Security breeches in one facility may affect others.

3.1 Administrative safeguards

Section 164.308 describes business processes that must be developed, deployed, and checked periodically to assure that medical information is properly safeguarded. This section explicitly requires handlers of medical information to perform risk analyses, risk management, document business processes, perform regular audits, and accept/assure accountability in an individual and organizational sense.

3.1.1 Risk analysis

Large institutions are at greatest risk for cyber attack for a number of reasons.

1. Large numbers of data transactions offer many opportunities for attack
2. Large institutions tend to be highly visible, and are more tempting targets for attack than smaller institutions.
3. Large institutions employ and interact with more people, and are more likely to dissatisfy one or more people to the point of provoking an attack.
4. Large institutions tend to handle more valuable information. Potential return on investment is greater for attacks on large institutions.

Small institutions tend to be vulnerable for different reasons. Small institutions often lack resources for investing in security, and sometimes provide staging areas for attacks on larger institutions.

The increasing inter-connectedness of medical institutions raises the risk of cyber-attack for all institutions, and strongly implies the necessity of increased investment in data security among all players in the industry. One way of considering the value of a network security system is to compare the cost of its installation with the legal cost of defending its absence when security is compromised. With this in mind, investment in information security is well justified.

Installation of Owl systems significantly hardens the security of any facility that anticipates a cyber-attack designed to steal or corrupt information. Owl systems satisfy numerous stringent security specifications in a cost effective way. Assurances that Owl systems provide benefits in IT security analyses include the following:

1. Owl systems carry the EAL4 certification, which is the highest level security certification found in commercial products.
2. Owl systems are deployed at numerous government agencies that handle the most sensitive and confidential information, including the National Security Agency (NSA), Central Intelligence Agency (CIA), and Defense Intelligence Agency (DIA).

Not all attacks are designed to steal or corrupt information. A large number of attacks are designed to overload an IT infrastructure with useless communications to the point where it no longer functions. These “denial-of-service” attacks are most difficult to defend against, and are a real threat. Owl systems are not intended for defense against denial-of-service attacks.

3.1.2 Risk Management

All Owl systems are based on hardware that is physically configured to pass data in one direction only. When properly configured, it is physically impossible for data to flow in the reverse direction.

There are many safeguards to assure that proper system configuration is achieved and maintained, which are described below. While Owl systems are primarily designed to reduce the risk of unauthorized data access through technical means of network communication, they are also packaged and deployed in a manner that minimizes risk of human error or malice through non-technical means.

3.2 Physical safeguards

Section 164.310 describes facility access, media handling storage & disposal, disaster recovery, computer platform configuration, and other concerns of a physical hardware nature. This section implicitly defines the physical characteristics of a secure information repository which is accessible only by authorized personnel. Physical safeguards describe how users may be authorized to enter the facility, and how such users may manage physical media on which information is stored and transported.

Owl systems are designed, manufactured, labeled, and deployed in a manner that makes installation easy and physical tampering difficult.

1. Individual Send and Receive cards are populated with components only for their specific function.
2. Cards and software CD-ROMS are marked in ways that are difficult to duplicate.
3. Cards must be matched with their respective software in order to function.
4. Network cards are designed for deployment in low-aspect rack-mounted computer platforms that conserve space in normal use and are not easily opened for tampering.

3.3 Technical safeguards

Section 164.312 describes management of users, passwords, encryption, firewalls, telecommunications and other IT concerns pertaining to logic and software. This section describes some of the technical details of how users may access information electronically, without physically entering the secure facility.

Owl's core technology provides a safeguard that significantly improves electronic access security by physically isolating electronic communications into one-way data transfers. Owl's core product connects two computers with an optical fiber that send data in one direction only at very high throughput rates (155 Mbps, OC-3). The sending end of the

fiber connects to a photoemitter. The receiving end of the fiber connects to a photodetector. Data can only be sent in the forward direction. It is physically impossible to send data in the reverse direction.

Owl systems are inherently fail-safe. Should the Owl system fail, the result is that no data can be transferred in either direction; an inherently secure state. To date (since 1998), no Owl system has failed in the field.

The nature of Owl systems significantly hardens the security of any facility that anticipates a cyber attack designed to steal or corrupt information.

3. Since no bilateral communication is possible across the one-way link, it is impossible to use software to probe for vulnerabilities on either side of the link.
4. IP routing is fixed at time of system configuration and cannot be reconfigured in a meaningful way without access to both Send and Receive machines; which requires physical access to the secure facility.
5. Since no network routing information passes across the one way link, it is impossible to construct a routing table from information stored in either the Send or Receive machine. Acquisition of complete routing information requires access to both Send and Receive machines, which requires physical access to the secure facility.

4 System Configuration Scenarios using Owl Products

This section describes a limited number of medical information processing scenarios where Owl one-way data transfer offers advantages in meeting data security standards.

Medical information is diverse in nature, and requires varying levels of security, depending on its nature. This implies that storage and transport of medical information requires a multi-tier approach to security as routinely encountered in military intelligence applications. Owl systems provide the capability for isolating data networks into varying levels of security appropriate for sensitive medical information.

Owl systems are most useful for high-throughput data processing scenarios where data can be “pushed” from the sending side of a network connection. General scenarios include

1. Accumulation of medical data in a secure centralized repository
2. replication of medical data from one secure repository to another
3. copying protected data from a secure repository to a read-only security area for controlled access

Specific scenarios where medical information can be pushed to/from a high security repository include the following:

1. Numerous geographically-distributed primary care clinics send examination data to a centralized facility with specialized expertise in diagnosis
2. Numerous geographically-distributed health care service vendors send billing data to a centralized financial services firm
3. Numerous health care service providers send archival data to centralized secure storage repository
4. Numerous health care service providers send scientific information to centralized public health institution.
5. A centralized public health facility exports scientific information of public interest to numerous geographically-distributed primary care clinics
6. Medical information clearing house posts information about the state of pending transactions from a high security repository to a read-only viewing area, where clients can track the progress of third-party payment.
7. Medical information clearing house exports anonymized medical information from high-security repository for actuarial analysis
8. Creation of medical documents (hardcopy) from any medical database or business process

We start with the description of a scenario in which medical data is accumulated at a secure central location from multiple users who are geographically separated. In this scenario, data is zipped and encrypted with passwords for sending across a Wide Area Network as shown in Figure 3.

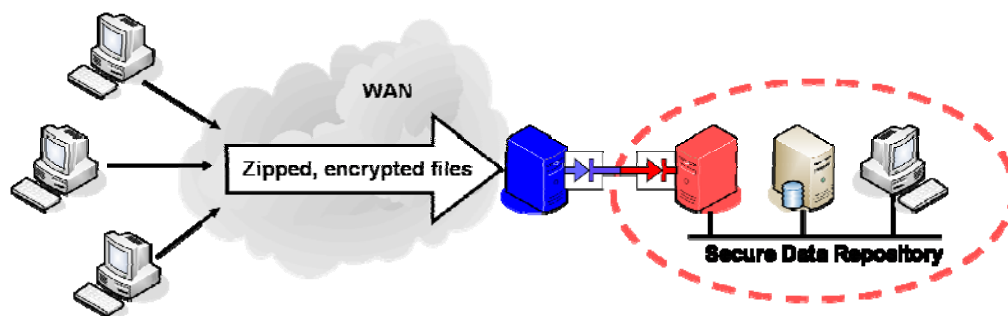


Figure 3: Remote users send medical data to central secure repository

Similar configurations allow medical data to be securely transferred from one high security zone to another high security zone as shown in Figure 4. As before, data may be zipped and encrypted with password for transport across wide area networks.

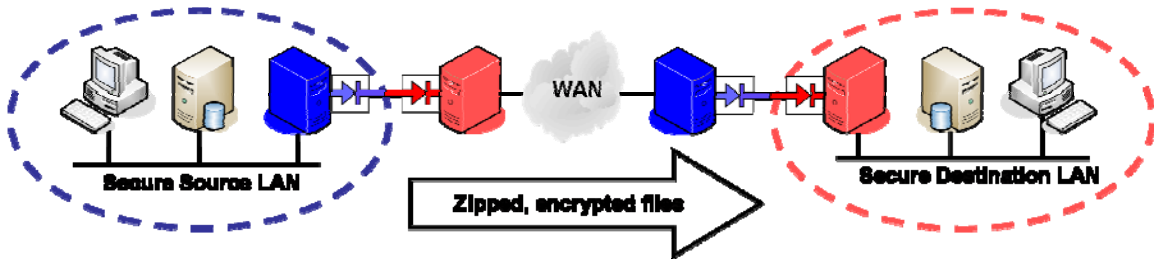


Figure 4: Data transfer of zipped, encrypted files from one secure network to another

A closely related scenario involves selective copying of information from a high security area to an intermediate security area for authorized users to gain read-only access as shown in Figure 5. This scenario is particularly useful for tracking medical data and medically-related financial transactions for active cases that are in process.

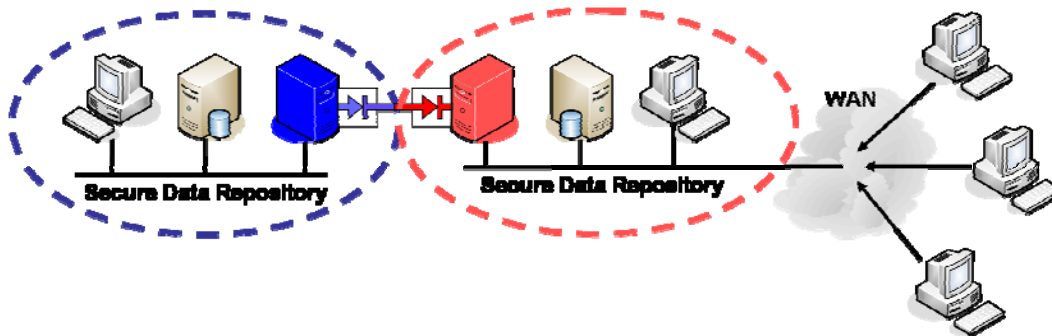


Figure 5: Secure medical data transfer to read-only access area

Another basic configuration allows medical data to be pushed from a secure repository to multiple locations in a controlled way as shown in Figure 6. This configuration addresses scenarios where trusted medical/pharmaceutical data must be disseminated in real time to numerous primary care facilities that are geographically separated. These scenarios include public health and disease control alerts, pharmaceutical data updates, and ABC warfare scenarios.

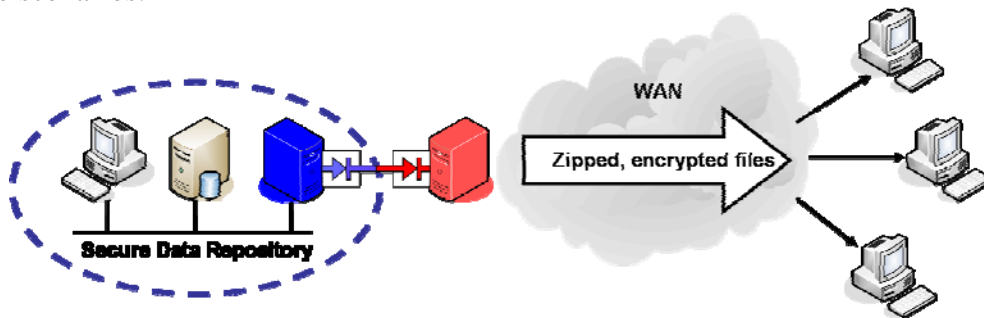


Figure 6: Controlled distribution of medical information from secure repository

It may be desirable to produce medical document hardcopy from data stored in a secure repository. Owl systems may be used to isolate the data repository from hardcopy output

stations; allowing a document to be printed to a non-secure area while denying any other form of access from that area, as shown below in Figure 7.

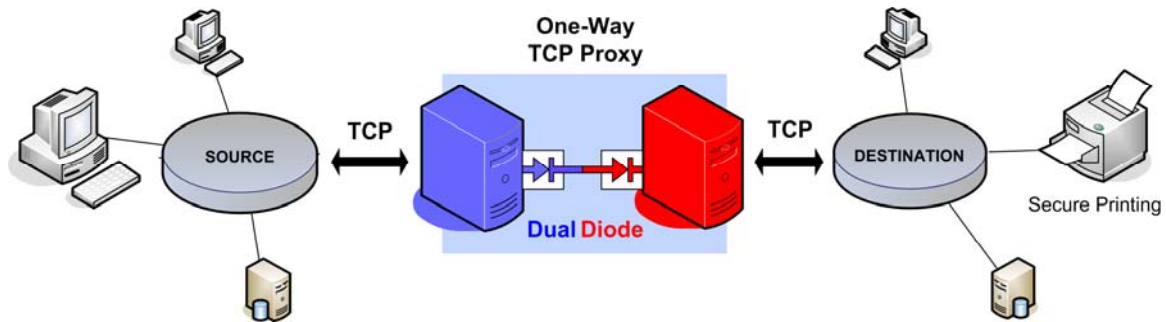


Figure 7: secure printing from protected network

5 Owl Systems in Context of Overall Network Security

While Owl's one-way Dual Diode data transfer technology is designed to significantly improve network security, it does not provide a standalone guarantee for network security.

Owl provides a fast and reliable one-way transfer mechanism that is known to improve network security and does not discriminate data. Owl products do not provide data content filtering or encryption. Owl products are designed for seamless integration with other security measures to prevent interception of data, transfer of malicious code, destruction or corruption of data, and denial-of-service attacks.

Any comprehensive security system must have in place a number of security measures to assure that data being transferred is valid, authorized, and not malicious. Overall network security cannot be achieved with any single commercially available product, or solely through technical means. Business process security rules, data content filters, access control lists, and other safeguards must all be deployed to assure integrity of data and network security in a larger context.

6 Conclusion

Owl Computing Technologies offers a secure one-way data transfer system that protects secure networks and provides significant benefits for medical IT architectures that transfer large volumes of information in electronic form. Owl systems satisfy numerous security specifications in a cost effective way, and are most useful for data processing scenarios where large data volumes data can be "pushed" from the sending side of a network connection.

7 References

http://www.access.gpo.gov/nara/cfr/waisidx_04/45cfr164_04.html

Code of Federal Regulation

<http://www.hhs.gov/ocr/hipaa/>

<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>

More Federal Regulations, with explanatory text

<http://www.commoncriteria.org>

http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf

<http://www.winzip.com/>

WinZip website; vendor of zip-encryption software

<http://www.pkzip.com/>

PKZip website; vendor of zip-encryption software

Health Care Financing Agency

<http://www.hcfa.gov/medicaid/hipaa/default.asp>

Health Care Information System Provider – IDX

<http://www.idx.com>

Phoenix Health Systems – IT Industry HIPAA Information

<http://www.hipaadvisory.com>

Microsoft Technet – Security

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp>

HIPAA Security – Richard Wark, Oracle Corp.

www.ehcca.com/presentations/HIPAA3/wark.ppt

<http://www.datadiode.com/>- Owl Computing Technologies Web Site

<http://www.anIP.com/>- AMP Web Site

<http://www.infineon1.com/>- Infineon Technologies Web Site

<http://www.jdt.com/>- Integrated Device Technology, Inc. Web Site

[1] Sandia Corporation. [1996]. Method For Transferring Data From An Unsecured Computer To A Secured Computer. United States Patent, us 5703562.

8 Revision History

| Release | Date | Changes / Reason for changes |
|---------|------------|--|
| 01 | 9/21/2005 | New document |
| 02 | 9/26/2005 | improved ordering of sections |
| 03 | 11/7/2005 | clarified description of data transport layer |
| 04 | 11/7/2005 | rewrote caveats section describing what Owl system is not. |
| 05a | 11/10/2005 | upgraded card photos |
| 05b | 3/16/2006 | improved wording of risk analysis section |
| 05c | 3/16/2006 | updated diagrams using Dual Diode icons |
| 05d | 6/21/2006 | upgraded Owl system network diagram, and inserted references for secure printing capability. |