

# Utah Environmental Public Health Tracking Program

Fall 2006

Issue 9

## *Security and the EPHT Network*

### Inside this issue:

Security and the EPHT Network	1
3 Layers of Security	3
System Security Definitions	4
EPHT Welcomes New Staff	5
Data Steward Q & A	5

**G**overnor Huntsman has declared October “Cyber-Security Awareness Month” for the State of Utah. The EPHT

Project staff are working to develop a secure network to share environmental health information. This newsletter is dedicated to discussing security, and how the EPHT Project plans on protecting the security of the EPHT Network.

All too regularly, reports of information technology (IT) security concerns appear in the news. Some are an accidental break down of security but most are the result of a malicious attack with the intent to do harm to the system. Maintaining the security of a data management information system is almost as much work as maintaining the data in the system.

A typical information system consists of a number of components, sometimes called layers by information technologists. Each layer is susceptible to security breaches that can cause harm to the system. For example, at the physical layer (the architecture of servers, hubs, routers and supporting hardware) the security of the system is dependent on the security of the physical environment in which it operates. That security can be disrupted by fire, water damage or hardware theft. To prevent security disruptions requires a closely monitored and controlled environment in a physically secure location.

At the data layer (the electronic storage of data on a server’s hard drive), security problems usually result because of data corruption. Data corruption can occur



because of a system failure (worn out hardware or an electrical surge, etc.) or by the malicious introduction of little programs (virus software) that are designed to delete, destroy, scramble or otherwise corrupt the data. One way to protect the data layer is to regularly archive the data and then store it at a different location. However, archived data is generally missing the last little bit of data obtained after the last archive. Another protection is to encrypt, or code sensitive data elements so only those with a set of instructions or “keys” can understand the data. Other vulnerable layers include the application layer, session layers, presentation layers, and data transaction layers. Each of those layers has one or more potential vulnerabilities that have to be managed through systems security policies and procedures.

### Special points of interest:

- October is “Cyber-Security Awareness month.”
- Find out how EPHT information is kept secure
- Viruses, worms, and more defined
- Questions and Answers for data stewards

Continued on Page 2...

## Security and the EPHT Network (cont.)

In addition to the system layer security concerns, the human element of a system can result in security threats that need to be addressed and managed. One only needs to recall the reports of potential loss of sensitive data about veterans when a well-meaning Veterans Administration employee took the data home (away from its physical security) on a laptop, only to have the laptop stolen from his home.

Information systems that use the Internet to transact data are particularly vulnerable. Attacks through the Internet can break into a system's application or data stores to examine, steal or destroy data. This kind of hacking is sometimes called an intrusion. A drastic response to an intrusion is a complete system shutdown. Attackers can also spoof the system, causing it to transmit data to an unauthorized recipient. Another type of attack seeks to overwhelm the system to such an extent that legitimate users can no longer access the system. This kind of attack is sometimes called "pinging to death," and results in a denial of services for other users. Spoofing and denial of service are more difficult to manage because the attack is not necessarily directly on the system. Once data has been released to the Internet, it is more difficult to control.

Typical security for an information system includes a number of policies and procedures. Policies should address such things as user access and responsibilities to the system as well as physical and systems monitoring or auditing. Policies may provide for the use of records tracing, archive cycles, and intrusion management.

Concerns about the increasing potential for "cyber terrorism" (terrorist attacks on national security and the economy through attacking information systems) have caused the national Department of Homeland Security to implement a series of robust and nationally consistent information security standards for all government information systems. The EPHT Network will be required to conform to those standards. During the implementation of the network, the Utah Department of Health will be working with the Centers for Disease Control and Prevention to acquire technology and to develop policies and procedures to implement those requirements for the Utah EPHT Network.

*For more information contact Sam Lefevre at [slefevre@utah.gov](mailto:slefevre@utah.gov) or Lew Jeppson at [ljeppson@utah.gov](mailto:ljeppson@utah.gov)*

In addition to the system layer security concerns, the human element of a system can result in security threats that need to be addressed and managed.

## EPHT Project Updates

The following are recent accomplishments of the Utah EPHT Project over the last few months.

### June

- EPHT Project demonstration of the Rapid Inquiry Facility (RIF) at the Council of State and Territorial Epidemiologists (CSTE) and the North American Association of Central Cancer Registries (NAACCR) annual conferences.

### August

- EPHT Project receives funding to implement the network.

- EPHT Project Staff makes three presentations and a poster exhibit at the National EPHT grantees conference.
- The Utah EPHT Planning Consortium becomes the Utah EPHT Technical Advisory Group (TAG).

### September

- EPHT Project Staff attend the Public Health Information Network Conference.

## Three Layers of Security

In order to better understand EPHT Network security, it is important to grasp how security measures function at each individual layer of a network. This article takes a look at security at the Internet, operating system, and application layers of a network. However, in administering security procedures one should be aware that all security is relative; no system is completely safe.

### Internet Security

Internet security is based on a protocol called Secure Socket Layer (SSL). Netscape developed this protocol for encrypted transmission over networks that move data as individual digital packets. These packets travel to the same destination point, but may be disassembled and go over different routes on the Internet. SSL has two functions: 1) It allows a client to verify the identity of a server, and 2) it enables secure two-way communication between a client and server. SSL is used on Web pages with forms that require passwords, credit card numbers, or other sensitive data.

When a Web-enabled computer program uses SSL, it listens on a second port for a connection and performs a handshaking sequence. This sequence establishes a set of "rules" for data exchange between computers. Once these rules are in place, the requested content may then be sent to the client.

Data encryption is another level of Internet security that prevents malicious users from eavesdropping on Internet connections and copying personal information. To encrypt communications, SSL sits between the network and an application and encrypts communications between the server and client.

### Operating System Security

Beneath the Internet we have internal network security such as Novell, which is an application to establish a local network for multiple computer systems. Utah state government agencies use Novell for the state local networks. A Linux computer operating system, which is Unix-based, may also be used. This level can become highly specific. Usernames and passwords are used while reading, writing and execution capabilities for various users can be specified to a high level of detail, particularly with Unix-based systems. On a Unix-based system only the system administrator has complete access. Everyone else is restricted to certain files. Unix systems are among the most secure of all multiple user operating systems.



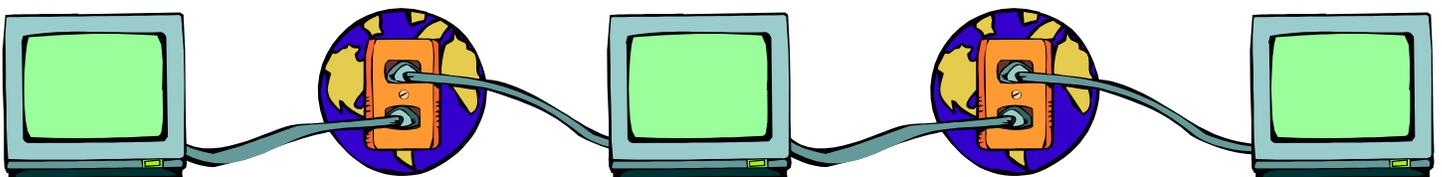
### Application Security

Beneath the operating system we have application (e.g., database vendor) security. This is a logical based security that restricts certain users of the database to certain files, applications and functions.

Security at every layer of the EPHT Network is a concern. We can ensure the reliability and utility of the information we provide by understanding the tools available for securing our data.

*For more information contact Lew Jeppson at [ljeppson@utah.gov](mailto:ljeppson@utah.gov)*

In administering security procedures, one should be aware that all security is relative; no system is completely safe.



## Information Systems Security: Some Definitions

### File Encryption

Unix systems often use a *crypt* utility to encrypt files. It is a good example of various encryption utilities. In general, encryption is a process of obscuring information to make it unreadable without special knowledge which acts as a “code.” In file encryption, the “code” is called the encryption key.

One may encrypt a file using the *crypt* command and then send it through e-mail, having informed the recipient of the encryption key. This is awkward, since you need to transmit the encryption key to the recipient separately from the message. A better solution to this problem is provided by public-key cryptography.

### Public-key Cryptography

In public-key cryptography there are separate encryption and decryption keys. Simply knowing an encryption key does not permit someone to determine a decryption key. With public-key cryptography you need only look up the public-key of the intended recipient in a public directory to encrypt a file that will be sent to this person. But only the recipients will be able to decrypt the transmission, since their decryption key is unique. Not only can you send files encrypted using public-key cryptography so only the intended recipient can decrypt them, you can also send signed messages, which indicate to the recipient that the message came from you.

### Secure Socket Layer

Secure Socket Layer (SSL) and the newer Transport Security Layer (TSL) are security protocols that use cryptography to ensure secure Internet communications such as Web browsing, email and other data transfers. Both protocols function similarly and the acronym SSL is often used to denote both protocols.



### Trojan Horses

A Trojan horse is a program that masquerades as another program or performs some other unintended action in addition to doing what the genuine program does. When a Trojan horse runs, it may send files to the intruder, change or erase files, or even collect information such as passwords.



### Viruses

Computer viruses and worms are relatively new types of attacks on systems. There is a strong analogy between a biological virus and a computer virus. A computer virus is a code that inserts itself into other programs and the programs are said to be infected. Computer viruses cannot run by themselves. A virus may cause an infected program to do some unintended action that may be harmful. One action of a computer virus is to have the infected program make copies of the virus and infect other programs and machines.

### Worms

A worm is a computer program that can spread working versions of itself to other machines. A worm may be able to run independently, or may run under the control of a master program on a remote machine. Worms are typically spread from machine to machine using electronic mail or other networking programs.

### Firewalls

All Internet or network services must be monitored to ensure that no one is trying to get into your systems over the network to perform mischief. The most common way to prevent this is to place a machine between your network and the outside world; this is called a firewall. The purpose of a firewall is to check incoming traffic to see if there are attempts to take information from, or to deliver information to the machines on your network by unauthorized outsiders. A variety of software may be used to construct a firewall.

There are a variety of threats to a computer network. However, there are also a number of security measures that can be taken to reduce these risks and build a secure, reliable network.

For more information contact Lew Jeppson at [ljeppson@utah.gov](mailto:ljeppson@utah.gov)

## EPHT Project Welcomes New Staff

The Utah EPHT Project is excited to welcome two new members of the project staff; Colleen Kelley and Adam Owens.

Colleen Kelly has joined the team as a data manager and she also works in geocoding. Colleen came to UDOH in January after spending nine years working as a software engineer in San Diego. She started her career in the Army, where she served for nine years and received a B.S. in Computer Science while in Belgium. She enjoys camping, hiking, fishing, knitting and crocheting.

Adam Owens has joined the team as a health educator and program-marketing specialist. Adam recently finished studying Public Health Education and Spanish at Brigham Young University. He likes skiing, climbing and hiking.



## EPHT Contacts

Wayne Ball, Principal Investigator  
[wball@utah.gov](mailto:wball@utah.gov)

Sam LeFevre, Project Manager  
[slefevre@utah.gov](mailto:slefevre@utah.gov)

Lew Jeppson, Research Analyst  
[ljeppson@utah.gov](mailto:ljeppson@utah.gov)

Brittney Carver, Technical Support  
[blcarver@utah.gov](mailto:blcarver@utah.gov)

Colleen Kelley, Data Manager  
[ckelly@utah.gov](mailto:ckelly@utah.gov)

Adam Owens, Health Educator  
[aowens@utah.gov](mailto:aowens@utah.gov)

## Questions and Answers: Data Stewards

### Q. What is a Data Steward?

Data Stewards include any organizations that are or may become data providers to the Utah EPHT Network. This means that the organization has environmental or health information that would be useful for environmental health tracking.

### Q. Why should data stewards provide data to the EPHTN?

The ability to access and analyze health and environmental data will increase the number and quality of the public health interventions that data can inform. The EPHT Network will be equipped with tools that may be useful for data owners or others who may access EPHTN data. Perhaps most importantly, the EPHT Project offers various data services to providers, such as geocoding.

### Q. Will data on the network be secure?

Data security is inherent within the structure of the national Public Health Information Network, within the framework of which state and national EPHT networks are housed.

### Q. Can stewards control what happens to their data?

Data stewards may develop a data use agreement that limits who can view the data and what can be done with it.

For more data steward information contact Adam Owens at [aowens@utah.gov](mailto:aowens@utah.gov)

## Future Activities & Important Dates

- **Technical Advisory Group (TAG) Meeting**  
Stay posted for information and the time and date of the next TAG meeting.

*If you have any events you would like posted in the next (winter) newsletter, please contact Adam Owens at [aowens@utah.gov](mailto:aowens@utah.gov).*



*Environmental Public Health Tracking Program*  
*Office of Epidemiology*  
*288 North 1460 West*  
*P.O. Box 142104*  
*Salt Lake City, Utah 84114-2104*  
*Phone: 801-538-6191*  
*Fax: 801-538-6564*  
[www.health.utah.gov/ephtp](http://www.health.utah.gov/ephtp)

---

WE'RE ON THE WEB [WWW.HEALTH.UTAH.GOV/EPHTP](http://WWW.HEALTH.UTAH.GOV/EPHTP)

---

## *Utah Environmental Health Tracking Program*

**Mission:** To develop a state-wide, standards-based, Web-enabled tracking network information system in Utah to enable information and knowledge dissemination and improve public health in the realm of chronic diseases related to environmental factors.

Contact Adam at [aowens@utah.gov](mailto:aowens@utah.gov) if you have an article or news you would like in the upcoming Utah EPHT newsletter

