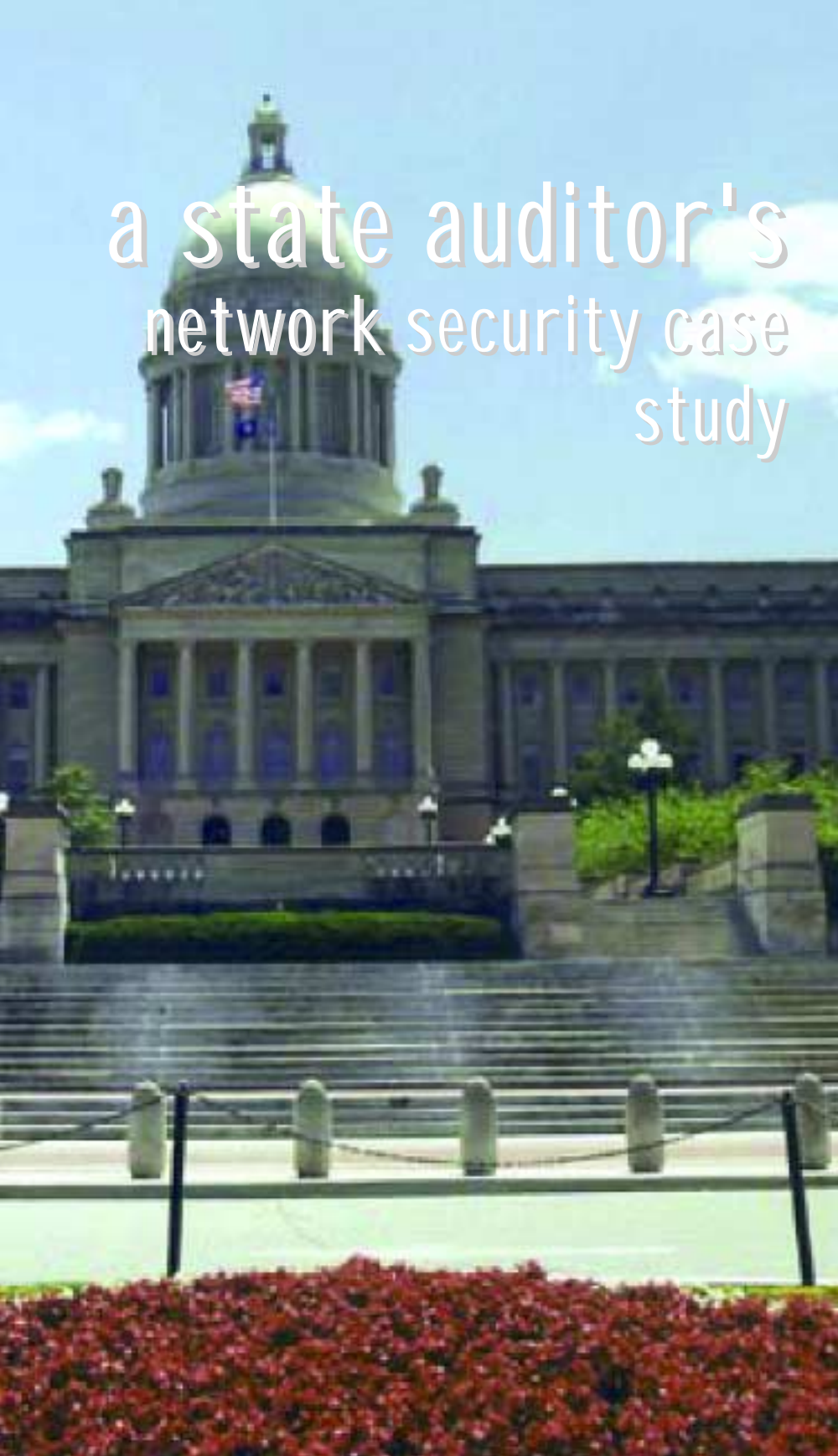


# a state auditor's network security case study



Capitol Building, Frankfort

The first vulnerability assessment performed by Kentucky's Auditor of Public Accounts tested the security of the Commonwealth's accounting and reporting system in June 2000. Within minutes, auditors were able to gain administrator control over 14 of 17 system servers. Thus began three years of random, surprise vulnerability tests in 16 state government cabinets and agencies.

## Vulnerability Assessment becomes Incident Handling in Kentucky's Transportation Cabinet

### Abstract

The Commonwealth of Kentucky's Auditor of Public Accounts began performing network vulnerability assessments in state agencies in June 2000. One such assessment performed in July 2003 revealed a significant, long-term intrusion during which hackers with French addresses broke into Kentucky's Transportation Cabinet network and used it to:

- Store and distribute pirated recently-released movies, music CDs and DVDs, TV shows, and new computer games;
- Post and distribute copyrighted French medical textbooks;
- Host an Internet chat room.

In addition, auditors found that Cabinet computers had been used to visit and view thousands of pornographic websites or images.

Auditors provided detailed evidence of the intrusion and misuse to Transportation Cabinet officials and state and federal law enforcement, highlighting for network administrators seven security issues, to wit:

- Persistent null passwords;
- Vulnerable administrative accounts;
- Compromised data;
- Password harvesting by hackers;
- Hacker-installed tools;
- Pirated copyrighted materials on servers;
- Widespread viewing of pornographic sites by system users.

Auditors recommended a variety of measures designed to strengthen user passwords, fortify firewalls, remove compromised machines from the network, assume tainted application and data back-ups, rebuild compromised machines from the ground up, refer forensic evidence to proper authorities, notify business partners and the public, and anticipate retaliatory attacks.

Network security weaknesses threaten taxpayer dollars and facilitate identity theft. Three years of performing vulnerability assessments leads Kentucky's Auditor of Public Accounts to conclude that (1) a universal formula such as ICAMP<sup>1</sup> for quantifying the economic cost of insecure government networks must be adopted, (2) accountability for network security is largely absent in Kentucky state government agencies, and (3) auditors must perform surprise vulnerability assessments and publicize their findings in order to have the greatest impact upon network security.

## Introduction

While auditors have performed information systems audits for many years, it was the Y2K alarm that foreshadowed a more systematic, focused inquiry on network security. Insecure government networks place taxpayer dollars at risk of cyber-theft and loss through network downtime. They also jeopardize the security of the unique identifiers like social security numbers and other confidential financial information of which government agencies are the repositories. Moreover, hackers may exploit insecure systems in the commission of other crimes. Known variously as ethical hacking, penetration testing, and vulnerability assessments, the procedures applied by auditors at every level of government have revealed alarming weaknesses, indifferent network managerial attitudes, and costly intrusions. Kentucky's Auditor of Public Accounts has performed surprise

assessments and publicized embarrassing findings to motivate government IT managers to give network security the priority it must have. Experience shows that if you exclude the element of surprise and the specter of adverse publicity, network insecurity may go undetected and important findings may be unaddressed, leaving systems unprotected.

*Common among the findings of the vulnerability assessments was an institutional failure to observe basic security principles. Perhaps the most basic security measure, the use of passwords, was frequently ignored or ineffective.*

The first vulnerability assessment performed by Kentucky's Auditor of Public Accounts tested the security of the Commonwealth's accounting and reporting system in June 2000. Within minutes, auditors were able to gain administrator control over 14 of 17 system servers. Following weeks of extensive consultations with network administrators, the assessment was re-performed in December 2000, revealing a significant strengthening of system security.

Thus began three years of random, surprise vulnerability tests in 16 state government cabinets and agencies. Each assessment produced both a written report of findings and recommendations for agency managers and contributed to a rising sense of alarm at the weak network security discovered throughout state government. During the first two years, the Auditor of Public Accounts refrained from publicizing assessment findings so as not to imprudently alert opportunistic hackers

to system weaknesses. As random testing continued, however, frustrating similarities emerged to reveal a government-wide inattention or indifference to network security. The Auditor of Public Accounts reluctantly concluded that raising public interest in the subject was essential to strengthening network security in government, and the office shifted toward making a public example of those agencies found to have disturbing weaknesses.

Common among the findings of the vulnerability assessments was an institutional failure to observe basic security principles. Perhaps the most basic security measure, the use of passwords, was frequently ignored or ineffective. In agency after agency, auditors found computers and servers with no password protection. Many administrator accounts were discovered to have null or weak passwords.

Another issue brought to light by the vulnerability assessments is the widespread belief by state government employees that network security is a responsibility reserved for the highest level of administrators. There is a mindset that network security is not a universal component in the job description of every network user. This rejection by network users of personal accountability for security has been fostered by the tendency of state

*The failure to implement internal controls is too costly not to implement, as was demonstrated in 1996 when the failure to properly employ and manage passwords allowed a five million dollar embezzlement in the Kentucky Revenue Cabinet.*

<sup>1</sup> Incident Cost & Analysis Modeling Projects... [www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml](http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml)

government systems managers to seek rational explanations, and make excuses, for insecure systems.

One such excuse refers to the democratic, open culture of government. Government's information systems are therefore logically open and accessible. Polemics aside, it is disingenuous to assert that prudent security measures should be compromised by fidelity to open government and transparency.

Cost is the most frequently cited impediment to network security, and to be sure, the latest architectural advancements in network security may require significant investment. Unfortunately, tight state budgets characteristically leave few, if any, dollars for security. Still, there are fundamental security measures and attitudes absent from Kentucky government agencies that require few additional resources beyond a commitment of reasonable diligence. For example, the Auditor of Public Accounts' work revealed a widespread failure of agency administrators to timely apply free downloadable system patches, resulting in significant, costly downtime when assorted viruses and worms attacked. Furthermore, auditors are quite accustomed to effectively rebutting the argument that internal controls are too costly to implement. The failure to implement internal controls is too costly not to implement, as was demonstrated in 1996 when the failure to properly employ and manage passwords allowed a five million dollar embezzlement in the Kentucky Revenue Cabinet.

Government managers seem surprisingly oblivious to the cost of insecure networks. It has been difficult, therefore, to get their attention. System crashes, downtime, and labor-intensive triage for compromised networks take a verifiable and meaningful economic toll, but network managers are often conflicted about revealing such problems and agency heads have no accepted formulae for calculating the losses.

The Kentucky Auditor of Public Accounts' vulnerability assessments during the last three years included two highly publicized findings that resulted in the issuing of separate *Auditor Alerts* to all state and local government agencies. In one such assessment, a randomly tested surplus agency computer was found, without password protection, to contain in clear text significant components of Kentucky's STD and AIDS database, including identities of those tested, their test results, and their sexual partners. An *Auditor Alert* advising effective methods of scrubbing the hard drives of surplus machines was issued.

In another assessment, a series of penetration tests was performed on agency wireless networks by "war driving." The ease of penetration led to issuance of an *Auditor Alert* discussing the special challenges posed to network security by wireless networks, including the widespread failure of network administrators to enable the security components of such systems. One unexpected collateral finding of this work was the absence of an effective firewall separating Kentucky's state government network from the University of Kentucky's network.

Tempered by this body of work, the Auditor of Public Accounts undertook a vulnerability assessment of the information systems in the Kentucky Transportation Cabinet in July 2003.

## Case Report

The Kentucky Transportation Cabinet's system is a centrally managed, enterprise class network, serving thousands of users at hundreds of remote sites, and interfaces with other state and federal networks. The system is used to manage massive road construction and maintenance projects, warehouse vehicle registration records, and house the personal, confidential information of licensees. It is directly linked to the Commonwealth's accounting and reporting system. The Transportation Cabinet's system uses industry standard rather than proprietary hardware and software.

As part of the audit of the Commonwealth's Comprehensive Annual Financial Report, the Auditor of Public Accounts performed a risk assessment of the Transportation Cabinet's information system. This assessment consisted of two activities: scanning and enumeration.

During the scanning phase, auditors used **fscan.exe**, **nmap.exe**, and **superscan.exe** to identify potential vulnerabilities among the Transportation computers and servers providing exploitable services such as web, telnet, and Microsoft shares.

Auditor analysis... led to the discovery of a malicious, on-going intrusion. This discovery transformed the auditors' vulnerability assessment into an incident-handling project where criminal activity was observed.....

- Hacker installed applications and services operating in stealth mode;
- A list of cracked administrative passwords;
- Gigabytes of data in daily transport;
- Harmful software stored on the system, e.g., netcat for creating covert backdoors, pwdump for extracting passwords, regedit for altering a system's registry, and prockill, for terminating procedures.



Kentucky Senate Chamber

During the enumeration phase, auditors used **enum.exe**, **net.exe**, and **nbtDump.exe** to analyze vulnerabilities identified by the scans. This enumeration highlighted (1) the existence of devices and user accounts lacking passwords, (2) version numbers of running programs, (3) user names and groups, including assigned privileges, and (4) unprotected Microsoft shares allowing privileged access to file systems of many computers.

Auditor analysis of one of the first vulnerabilities that came to light during enumeration led to the discovery of a malicious, on-going intrusion. This discovery transformed the auditors' vulnerability assessment into an incident-handling project where criminal activity was observed.

The following hacker exploits were observed:

- Hacker installed applications and services operating in stealth mode;
- A list of cracked administrative passwords;
- Gigabytes of data in daily transport;
- Harmful software stored on the system, e.g., **netcat** for creating covert backdoors, **pwdump** for extracting passwords, **regedit** for altering a system's registry, and

**prockill**, for terminating procedures.

Auditors acquired irrefutable evidence that these programs, and several others, had been used. They observed hackers actively managing their ownership of the system, and unauthorized persons uploading and downloading pirated multimedia software. This material included (1) pirated new release movies, music CDs, DVDs, TV shows, and new computer games, and (2) newly copyrighted French medical textbooks.

Included in the hacker configuration files and documentation was the following statement, in clear text French. Auditors used *babelfish.altavista.com* to produce the following translation:

- This server was hacké by SuBy on request of a person. SuBy declines any responsibility towards this person and could not be held for person in charge for though it is;
- This server does not exist 2) all this Of course is legal ;D 3) SuBy rox 4) racism No (ouai C rare I C ;p) 5) the 1337 are not authorized 6) the files are has an informative title ;D 7) the hackers could not be held for persons in charge! 8) the files must be unobtrusive in the 24 hours 9) \$\$\$--- IT IS NECESSARY TO OBSERVE the RULES ---\$\$\$;

- We wish you a pleasant stay on this pubstro;
- Thank you has all those which make live the French scene.

Among the hacker configuration files and logs, auditors observed 25 IP addresses of intruders. Using McAfee's **neotrace** program, auditors traced these addresses to their geographic points of origin in France, Croatia, and Canada. They also found that a remote Internet relay chat room was being controlled by **eggdrop**, a hacker program residing on a Transportation Cabinet server. This allowed the hackers to control admittance to the chat room and to exploit the anonymity it provided.

Unrelated to the intrusion noted above, auditors discovered web proxy logs detailing the browsing habits of system users. A cursory examination of these logs revealed that several hundred computers were used to visit several hundred unique, pornographic websites in violation of the Commonwealth's acceptable use policies governing information technology systems. The auditors chose to focus on pornographic site browsing because such sites are known to be a disproportionately large source of malware, software intended to compromise a visitor's computer or system. Such attacks go largely unreported by victims because they are self-incriminating.

Later, more detailed analyses of the web proxy logs indicated the intentional, persistent browsing of websites displaying pornographic images of children. Some 34 computers were found to have been used to search for and access child pornographic material. The findings were promptly referred to state and federal law enforcement.

For two weeks, auditors performed their scanning, observing, and evidence gathering undetected, even though no attempt was made to mask the activities.

## Conclusion

The Auditor of Public Accounts found Kentucky's Transportation Cabinet network to be inadequately protected and unmonitored. While firewalls, activity auditing software, content managing software, and intrusion detection systems were in place, none was being used effectively, and some not at all.

Auditors recommended a variety of measures designed to recover from the malicious intrusion and establish effective defenses. The detailed findings of the vulnerability assessment and its accompanying recommendations were communicated to the Transportation Cabinet prior to public disclosure. The recommendations included:

- Applying strong passwords;
- Enabling and fortifying firewalls;
- Removing compromised machines from the network;
- Working from the assumption that application programs and data backups are tainted;
- Rebuilding compromised machines from the ground up;
- Quarantine compromised machines and make them available for forensic analysis;
- Notifying business partners and the public;
- Anticipating retaliatory attacks;
- Installing network sniffers to detect traffic to or from previously identified hacker addresses.

Network security weaknesses threaten taxpayer dollars and facilitate identity theft. Three years of performing vulnerability assessments leads Kentucky's Auditor of Public Accounts to conclude that (1) a universal formula such as Incident Cost and Analysis Modeling Projects, ([www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml](http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml)) for quantifying the economic cost of insecure government networks must be

adopted, (2) accountability for network security is largely absent in Kentucky state government agencies, and (3) auditors must perform surprise vulnerability assessments and publicize their findings in order to have the greatest impact upon network security.

Edward B. Hatchett, Jr.,  
Auditor of Public Accounts,  
Commonwealth of Kentucky

<http://www.kyauditor.net>  
e-mail to... [ED.Hatchett@KYAuditor.net](mailto:ED.Hatchett@KYAuditor.net)

B.J. Bellamy, SANS GSEC, GCIH, GCFA,  
Chief Information Officer



**Lincoln Statue, Capitol Rotunda.**

Abraham Lincoln was born in Hodgenville, Kentucky, and served as the 16th president of the United States.

## The Commonwealth of Kentucky

Originally part of Virginia, the land that is now Kentucky became Kentucky County in 1776 and the fifteenth of the United States in 1792. The use of "commonwealth" doesn't have any particular significance, being a term commonly used in the eighteenth century meaning the same as "state".

Kentucky covers a land area of 40,395 square miles (104,623 sq km) and has a population of just over 4 million people. The State is divided into 120 counties, its capital Frankfort being in Franklin County. Kentucky's state constitution was adopted in 1891. The Governor is elected for a term of four years, the General Assembly, or legislature, is bicameral, with a senate of 38 members and a house of representatives of 100 members. Kentucky is represented in the U.S. Congress by six representatives and two senators, and has eight electoral votes.

Within the Commonwealth's Constitution, the role of the Auditor of Public Accounts is to ensure that public resources are protected, accurately valued, properly accounted for, and effectively employed to raise the quality of life of Kentuckians. Within the State Audit Office, the Information Technology Branch audits government computer systems and the data they generate. The branch also produces auditable information for financial and performance auditors by extracting, analysing, and reporting data derived from agency computer systems.

*Editor*

Kentucky Legislature Home Page.....  
<http://www.lrc.state.ky.us/home.htm>

Kentucky Constitution.....  
<http://www.lrc.state.ky.us/Legresou/Constitu/intro.htm>