AFRL-IF-RS-TR-2005-395
Final Technical Report
December 2005

ADVANCED NETWORK SECURITY PROJECT

Indiana University

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-395 has been reviewed and is approved for publication

APPROVED: /s/
ANDREW J. KARAM
Project Engineer

FOR THE DIRECTOR: /s/
WARREN H. DEBANY, JR.
Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
December 2005

3. REPORT TYPE AND DATES COVERED
Final Sep 02 – Sep 03

4. TITLE AND SUBTITLE

ADVANCED NETWORK SECURITY PROJECT

5. FUNDING NUMBERS
G - F30602-02-2-0221
PE - 06060F
PR - IANS
TA - A6
WU - 10

6. AUTHOR(S)

Steven Wallace, Gregory Travis, Edward Bates, David Ripley

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Indiana University
400 East Seventh Street
Bloomington IN 47405

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/IFGB
525 Brooks Road
Rome NY 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TR-2005-395

11. SUPPLEMENTARY NOTES
Andrew J. Karam/IFGB/(315) 330-7290 Andrew.Karam@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*

Indiana University's Advanced Network Management Lab entered into a contract with the United States Air Force for the implementation of a two-year program to study operational cybersecurity issues on a large, high-speed, digital network. The network observed was the Abilene network of the University Consortium for Advanced Internet Development (UCAID), often known as "Internet2". This contract was heavily operational in nature, as opposed to a contract with a specific research goal and hope-for outcome. Much of the work involved setting up systems and procedures for the active monitoring of the Abilene network and then the reactive reporting of observed activity.

14. SUBJECT TERMS
Incident response, Indicent database, Abilene

15. NUMBER OF PAGES 10

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

1 Introduction

Indiana University's Advanced Network Management Lab entered into a contract with the United States Air Force for the implementation of a two-year program to study operational cybersecurity issues on a large, high-speed, digital network. The network observed was the Abilene network of the University Consortium for Advanced Internet Development (UCAID), often known as "Internet2."

This contract was heavily operational in nature, as opposed to a contract with a specific research goal and hope-for outcome. Much of the work involved setting up systems and procedures for the active monitoring of the Abilene network and then the reactive reporting of observed activity.

A software development role was also specified, with the goal of investigating and developing tools for the monitoring and mitigation of cybersecurity incidents. The software developed under this contract is included as a separate part of this report deliverable.

An educational mission was attached to the contract, to be fulfilled primarily in two large annual cybersecurity workshops. These workshops were performed in the summer of 2003 in Indianapolis, Indiana and the summer of 2004 in Bloomington, Indiana and were open both to the sponsoring agencies as well as to the general public. The course materials generated and distributed as part of the workshops is also included as a separate part of this report.

Finally, regular reports were generated congruent to the deliverables of the contract. These consisted both of regular monthly reports on operational observations, included as a separate part of this report, as well as two larger reports given in response to two significant cybersecurity events. Those reports are also included as a separate part of this report.

2 Summary and Activities Performed

The contractor tasks specified included the following:

- Incident Response Analysis and Research
  - This is the primary operational activity covered under this contract and included:
    - Leveraging the differences between Abilene and other research networks, particularly high-speed networking and IPv56
    - An assessment of those Distributed Denial of Service (DDoS) tools already available for Abilene
    - Research the detection and response capabilities of Abilene
    - Research attacks against the Abilene core infrastructure
    - Identification of the ingress and egress of "bad traffic" through Abilene
- Establishment of an Incident Database
  - This was also an operational activity and consisted primarily of the following:
    - The specification and maintenance of an approximately 1TB database storing operational "NETFLOW" data.
    - Programs, scripts, schemas, etc. for the storage and manipulation of that data
    - Programs, scripts, etc. for the analysis of that data
- Tool development
  - In addition to the tools developed to facilitate the mission of Incident Response Analysis and Research, additional stand-alone tools were developed, particularly for the deployment of Honeynets and both active and passive forensic wiretap capabilities using the Sebek system
- Knowledge Transfer
  - This was accomplished primarily through the two summer workshops

3 Results and Discussion

Over the term of the contract, the following was observed:

The network constantly transited and sourced various forms of cybersecurity issues, particularly DDoS events. These issues and activities can be considered chronic to any reasonably sized digital computer network. The vast majority of the activity consisted of “nuisance” traffic, usually generated automatically by software robots.

Calibrating the point below which this undesirable activity should be ignored and the point(s) above which human action should be taken is exceedingly difficult. As part of the contract’s activities, we evaluated various automatic mitigation technologies (i.e. SNORT, Arbor, etc.) and concluded that all were incapable of unattended, stand-alone, “fire and forget” behavior. In those modes all of the existing software systems produced unacceptable failure modes.

One conclusion reached was that, in general, the networks themselves are not vulnerable to cybersecurity issues (the exception being the type of attack which generates network state in network operational elements, such as routers – this type of attack is detailed in the enclosed SQL Slammer report). Instead, high-speed digital networks serve as delivery devices, delivering harmful payloads to end-systems.

It is therefore likely that the most fruitful efforts at issue mitigation will be those efforts concentrated on end systems, as opposed to mitigation at the network level. Examples of end-system mitigation techniques and forensic tools include the Sebek technology developed under this contract. More on Sebek is to be found in the included presentations, the included software, and in the included periodic reports.

Of significant note is the degree to which homogeneity of both hardware and software systems facilitates both the spread of cybersecurity incidents and the scope of damage possible. The prevalence of a single, dominant, desktop operating system technology was observed as the greatest facilitator of worm, virus, etc., spread and impact.

Likewise, that much of the network core hardware and software technology is confined to a handful of vendors and vendor’s technology also provides an opportunity for significant disruption from a relatively small and unsophisticated type of attacks. Both of these situations are described more in depth in both the SQL Slammer and the MS BLASTER reports enclosed.

Finally, it was observed that new technologies, even those invented or designed to mitigate cybersecurity incidents, involve inherent dangers. For example, it was observed that the increased deployment and mandated use of the IPv6 protocol was likely, and in fact had, increased the exposure and liability of computer networks and end-systems, instead of decreasing those as had been a primary advantage initially touted.

Because new implementations always carry with them new vulnerabilities, the deployment of any new technology carries with it a risk period as the vulnerabilities are discovered, exploited, and eventually mitigated and eliminated.

4 Recommendations

As a result of our experience during the conduct of this contract, we make the following recommendations:

- As much as is possible, cost and efficiency issues involved in the design and procurement of networks and end systems be subrogated to a consideration of system heterogeneity. As wide a variety of vendors and technologies as is possible, given mission constraints, should be presumed over other considerations. Discontinuities in system design, vendor, etc. provide natural firebreaks and give significant advantage in halting the spread and impact of damaging events, such as worms, viruses, and system "bugs."

- Concentration move from networks as the loci for the mitigation of DDoS events and towards end-systems. In general, we observed that the network level was a poor place for observation and mitigation for the following reasons:

    - There is always a large amount of DDoS and other type of activity present in any large network. It is simply not practical to separate the truly damaging form of this activity from benign (though illicit) activity. The network provides the aggregation point of all licit and illicit traffic and, as such, it is the place where it is perhaps most difficult to see the "forest for the trees"

    - The cost drivers, motivations, and accountability metrics used to evaluate network operations are not conducive to cybersecurity mitigation. Networks make money when they move bits, not when they impede them (through firewalls, etc.) A network transiting a large DDoS event will nevertheless usually be operating entirely normally (i.e. the network itself will not be damaged by the DDoS event) and therefore no motivation accrues to the network's operators to mitigate the events.

- More effort and resources should be directed at the end-system problem. This problem takes the following form:

    - Balancing flexibility and programmability of the end-systems against possible vectors for attack

    - Providing forensic tools for the monitoring of end-systems while considering privacy and legal issues around such monitoring

- The correlation of simultaneous activity on multiple end-systems so that accurate and rapid “tracebacks” can be performed. Because of the international nature of most networking, it is not possible to rely on traditional methods (i.e. traceroute, ping, etc.) of sourcing attacks. Systems need to be deployed at national borders (for example) that facilitate the correlation of simultaneous outbound and inbound traffic.