DATA ON SCIENTIFIC COLLABORATORS

1. Faculty Associates:

- Dr. Geroge Harrison, Full Professor of Computer Science (worked from July 1998 through May 2000) – focused his investigation on digital encryption. Although encryption is generally relatively transparent to the user, often decisions must be made in procuring security software that effect the tradeoffs of speed of transactions versus degree of security needed. His findings were included in the "Web Security Starter's Kit for **Wired** Data Networks".
- Dr. Prathap Basappa, Assistant Professor of Computer Science - (worked from September – December 2000 at no additional cost to the sponsor) looked into interference issues to wireless transmission and WAP. His findinds were included in the "Web Security Starter's Kit for the **Wireless** Data Networks, v1.0 (the Wireless Kit) "

2. Research Assistants (Undergraduate Students)

- Mr. Randolph Martindale- hired during Phase I & a part of Phase II (July 28, 1998 – May 1999) to install and maintain the Web servers, proof-read the UNIX System Security part of the Kit and test the default security configuration of Apache Server running on ReHat Linux 5.2 His findings were included in the Phase I & II reports
- Mr. John Francis – hired during Phase II (June – Dec. 1999) to verify all the Security Starter's Kit against various configurations of NT workstations and servers, including applying various service packs. His findings were included in the "Web Security Starter's Kit for Wired Data Networks"
- Mr. Larry Scroggins – hired during the Spring Semester of Phase II (January 1999 – May 1999) to verify the security configurations of Linux systems and servers.
- There were no suitable students for Summer of 2000.
- Mr. Matthew Sanders (hired Sept. 2000 – April, 2001) and Mr. Michael Williams (hired Sept. – December 2000) – worked during Phase III to organize NSU Network Security Interest Group and set up a network security testbed to
  a. Test the security configurations of NT as well as Linux systems,
  b. Learn to conduct intrusion detection testing

TECHNICAL SUMMARY

The project is completed in three (3) Phases:

- Phase I investigation originally set from July 23, 1998 to January 22, 1999.
- Phase II investigation originally set from January 23, 1999 to January 22, 2000.
- Phase III investigation originally set from January 22, 2000 to January 21, 2001. At the request of the Principal Investigator, a no-cost extension was given to extend it till April 20, 2001. The extension allowed us to support a research assistant completing his additional responsibility of organizing a network security interest group to test the Web Security Starter's Kit.

The grant administrative activities include: grant financial account setup, student research assistant recruitment, equipment, software and book acquisition, lab facility management, monthly progress meetings, and monthly financial statements checked, and filing all reports to the Sponsor.

Documents submitted with this Summary are

1. Web Security Kit for Wired Data Networks
2. Lecture notes from the 5-day Web security workshop
3. Web Security Kit for Wireless Data Networks

1. Accomplishment in Phase I

The Investigative activities conducted in Phase I include the followings:

1.1 Grant Administration (Dr. Kung)

- Norfolk State University Grant account setup for Phase I grant and grant renewal for Phase II.
- Student Research Assistant selected in July, 1998 and new student Research Assistant (RA) selected to assume the vacancy in May, 1999 after the current RA graduates.
- Secretarial Assistance obtained
- Monthly financial statements checked
- Monthly team meeting held, and progress checked
- Weekly meeting with the RA, and progress checked
- Incremental progress status reported to Mr. Michael Vu, FFA technical point of contact on December 11, 1998 and January 27, 1999
- Phase II Plan of Work was drafted by Dr. Harrison and Dr. Kung, discussed with Mr. Vu.

1.2 Equipment Purchased (Dr. Kung)

The equipment and software were purchased and installed to provide 3 different popular Web host platforms for testing: UNIX (IRIX), LINUX and Windows NT, described as follows.

- An SGI O2 MIPS R5000 workstation with 340 MB RAM and 13 GB Disk was purchased and the WebForce package was installed.
- A Gateway 2000 PII-350 with 128 MB RAM and 6 GB Disk was purchased and the Windows NT server, and the Microsoft Internet Information Server were installed.
- The RedHat Linux system and the Apache server were installed on an existing IBM PC 365 (Pentium Pro 180, an existing Lab Equipment)

1.3 Industrial Partnership (Dr. Kung)

Although the investigation on the Wireless Data Network does not commence until Phase III, initial contact has been made with Lucent Technologies, an industrial supporting partner under this Project. Dr. Kung (PI) was invited for an expense paid visit to Lucent Technologies at Naperville, IL from May 20 to 22, 1998. During the visit, he met Mr. Howie McDonnell, Director of Wireless New Project Development and had lengthy technical information interchange with Mr. Antonio Ransom, a member of the Technical Excellence Team. More specifically, the CDMA wireless handoff protocol and security issues were discussed. More visits will be scheduled in the future.

1.4 Security Conference Attended (Dr. Kung)

Funded partially from the travel money ($1,000) provided by this grant, Dr. Kung attended the Fourth Annual UNIX and NT Network Security Conference sponsored by SANS from October 24 to 31 at Orlando, Florida. New types of system and network intrusions and their counter measures were reported. Dr. Kung also purchased security literature and CD at the Conference. Information gathered will be included in the proposed security guide.

1.5 Investigation Organized. (Dr. Kung and Dr. Harrison)

Different investigative topics were assigned to Dr. Kung (PI) and Dr. Harrison (FA) as shown in the following draft of the Web Security Starter's Kit (the Kit). Mr. Randolph Martindale (Research Assistant) was tasked to install and maintain the Web servers, proof-read the UNIX System Security part of the Kit and test the default security configuration of Apache Server running on ReHat Linux 5.2 All finding are included in the first Draft. (Not included here)

2. Accomplishment in Phase II

2.1 The "Web Security Starter's Kit for the Wired Data Networks, v1.0" (the "Kit") was completed in 1999 as scheduled. A subsequently updated version 1.1 was completed in January 2000 and submitted to Mr. Michael Vu, FAA Technical Monitor. The Kit along with final reports from previous project sponsored by FAA was placed on the Web (http://www.cs.nsu.edu).

2.2 Conferences and Seminars - The success of this Kit generated some interest from the academia. Subsequently, several workshop, tutorial and seminars were given by Dr. Kung on the security related topics to include:

- "Web Security for Small Web Sites", Tutorial Presenter, 1999 International Computer Science Conference, Hong Kong, Dec 16, 1999
- "A Web Security Guide for Laboratories" workshop Presenter, FIE99 (Frontier in Education) Conference on e-commerce, Nov 10, 1999
- Invited Seminar Talks
  a. "Web Security Practices", and "Research Problems on Web Security", Department of Computer Science and Technology, Peking University, China, Dec 23, 1999
  b. "Research Problems on Web Security", Department of Computer Science and Technology, Tsinghua University, China, Dec 24, 1999,
  c. "Web Security Practices", Computer Science Seminar, Norfolk State University, Nov 1999

2.3 Dr. Kung (Principal Investigator) attended a few security-related conferences to update his knowledge and exchange information with attendees:

- The 8th International World Wide Web Conference at Toronto, May 7 - 13, 1999. He attended a pre-conference course on "Distributed Object Security for Web-Based Application" and the e-commerce and XML security tracks to gather information for the Web Security project.
- Web 99 Conference in San Francisco, 1999.
- SANS 99 in New Orleans, 1999

2.4 Dr. Harrison (Faculty Associate) continued his investigation on digital encryption. His findings were summarized in APPENDIX B. Dr. Kung investigated wireless communication protocols (e.g. WAP, Wireless Application Protocol and Bluetooth), security in distributed computing, and XML digital signature. Findings were included in Phase II Report.

3. Accomplishment in Phase III

3.1 The "Web Security Starter's Kit for the **Wired** Data Networks, v2.0" (the Kit) was updated (attached to this report submission). This updated version includes a section on the intrusion detection.

3.2 The "Web Security Starter's Kit for the **Wireless** Data Networks, v1.0" (the Wireless Kit) was completed. The adoption of wireless web in the U.S. has been slow and there are few reported incidences. However, we believe that the wireless web will become the next playground for hackers. At no additional cost to the Sponsor, Dr. Prathap Basappa, our new Faculty Associate with a Ph.D. in EE, wrote the Appendix in which he reviewed the basic wireless technology and pointed out areas where potential vulnerability may occur.

3.3 The success of the Kit continues to generate interests from the academia. In addition to two invited lectures in December of 1999, several other invited workshops and seminars were given by Dr. Kung on the security related topics to include:

- A 5-day workshop on "Web Security Practices", Department of Computer Science and Technology, Tsinghua University, China, Aug 7 – 11, 2000,
- "Web Security Practices", Computer Science Seminar, Loayang Institute of Technology, Honan, China, August 14, 2000
- "IP-Spoofing", NSU Network Security Interest Group Seminar, Oct 2000

3.4 Dr. Kung (Principal Investigator) attended two security-related conferences this year to update his knowledge and exchange information with attendees:

- SANS SNAP 2000 in San Jose, CA, May 8 - 12 2000
- Attended LISA Conference Win 2000 Security Workshop, Seattle, WA, Aug 2000

3.5 Dr. Kung passed the SANS GIAC Certified Intrusion Analysts (GCIA) exam and received his 4-year certificate, June, 2000 (http://www.sans.org/y2k/analysts.htm)

3.6 Under the supervision of Dr. Kung, computer science students have organized the NSU Network Security Interest Group. The Group meets weekly and was assigned study topics such as intrusion detection activities using network security tools such as TCPDump, Snort and NMAP. The Research Assistants provide the leadership to the Group and manage a security research facility of three networked computers.

3.7 In the area of curriculum development, Dr. Kung designed a new course in "System and Network Security" to be offered in the Spring of 2001. In addition, a professional certification and curriculum development proposal was submitted to National Security Agency for funding.

4. Findings on XML Related Security Issues

Our investigation on the security issues related to XML documents was proven important recently with the introduction of UDDI (Universal Description, Discovery and Integration), an industrial effort (http://uddi.org) to standardize the interface to the web service discovery and access. The remote web service access defined in UDDI is exactly the Simple Object Access Protocol (SOAP) that this PI predicted in the computer science seminar held in Tsing Hua University and Peking University last December. The SOAP protocol invokes remote services on web by using the HTTP protocol to pass an XML document that encapsulates remote procedure calls and their parameters. In the past, CORBA, though a powerful distributed computing paradigm, remains too complicated, and expensive to deploy. CORBA can only find limited success in an intranet environment. Microsoft DCOM (ActiveX) technology never took off because of its platform dependent nature, can only find limited success in intranet of Windows systems. Since web servers are exposed to the Internet and the TCP port 80 for the HTTP protocol is typically permitted to pass through firewalls, SOAP becomes the only viable choice by default. SOAP seems to be a good compromise that may become successful in turning the Internet in to a big distributed computer. Therefore, a continuing examination of the SOAP protocol and implementation shall be the next area of security interest for the near future.