Security Plan for Red Team Testing

Matt Bishop, Principal Investigator, University of California, Davis

1. Introduction

The goal of the security plan is to ensure that proprietary and confidential information remains proprietary and confidential. Compliance with this plan is mandatory for all participants in the red team testing portion of the project.

In what follows, "proprietary" means that the vendor and the Secretary of State agree that the information or device is proprietary, for example source code. "Sensitive" means the information relates to the attacks, testing, and reports about the testing. Please use common sense here. Remember, the statement of work says:

> No Principal Investigator, UC Senior Reviewer, Associate Reviewer or accessibility expert shall make or release any comments or other information about the processes, procedures, progress or findings of the voting system review or any draft or final report to any third party via any medium for 45 days from the submission of the final report to the SOS, or until the final report is made public by the SOS, whichever is sooner. (p. 9, Scope of Work, Agreement No. 06158101)

2. Secure Facilities

We are planning for two types of secure facilities. The first type is at a remote institution, and is to be used for planning and preparation. The second, at the Secretary of State's office, is where all testing will take place.

2.1. Remote Facility

This facility is to be used for planning attacks and preparing for the testing. No e-voting systems will be sent to these facilities, but source code and proprietary documents may be sent there. These sites shall follow the "Security Plan for Source Code Review Teams", appended.

2.2. Secretary of State's Secure Facilities

All testing will take place in the secure facilities provided by the Secretary of State. The Secretary of State has primary responsibility for providing security. Participants will abide by any rules that the Secretary of State deems necessary. Access to the room will be limited to project participants, and others for whom the Secretary of State may allow access. The Secretary of State may also allow remote observers using video technology.

The room will contain two types of systems.

1. The first set of PCs will be connected *only* to an internal network. These will be called "red PCs" and will be identified by red tags or tape. Proprietary and sensitive information may be installed on these PCs. They will be on a network internal to the secured facility; this will be called the "red network".
2. The second set of PCs will be connected *only* to an external network via a DSL line. These will be called "green PCs" and will be identified by green tags or tape. These machines are to be used to retrieve information or software from the Internet as needed. They are *never* to be

connected to the red network, and are not to have source code, documents, or red team reports or drafts on them.

If something is to be moved from a green PC to a red PC, a removable disk (such as a CD) or drive (such as a memory stick) is to be used. Before it is connected to the green PC, the medium is to be wiped in a secure mode. Once it is plugged into, or mounted onto, a red PC, the medium is not to be attached to or put into a green PC until it is securely wiped, unless it is being used *only* to transfer encrypted data to a PC for mailing, as permitted in Section 5. The removable disks and drives used for this purpose are to be tagged with blue labels or tape.

Summarizing, the colors are:

- ***Red***—sensitive information such as source code, proprietary documents, and so forth, and the systems, devices, and networks on which they reside.
- ***Blue***—removable drives or memory sticks used to move data from the green network or devices to the red network or devices
- ***Green***—non-sensitive information, and the systems, devices, and networks on which they reside.

All cabling, and any external accessories to the systems (such as removable media) is to be clearly labeled red, green, or blue as appropriate.

The red and green networks are to be separated by an air gap. This will prevent any accidental transfer of information from the red to the green network.

3. Procedures

The following procedures will be observed:

1. All reports, source code, and any other sensitive information is to be stored on the internal PCs. only. Anything on which any of this information is stored is to be labeled red immediately. In particular, this information may *never* be stored on anything labeled green or blue.
2. Under no circumstances will anything labeled red be attached to anything labeled green.
3. Anything labeled blue must be securely wiped before it is connected to anything green.
4. No proprietary documents, source code, laptop, or anything labeled either red or blue is to be removed from the secured facility.
5. Any paper documents containing proprietary or sensitive information are to be shredded when no longer needed, or at the end of the project, whichever comes first.
6. Any network application may be installed on the internal or Internet PCs. However, under *no* circumstances will the applications communicate from the red to the green network, or *vice versa*.

4. Communication with Other Teams

Team members may communicate over the Internet with other project participants about proprietary or confidential matters ***only*** in the form of email encrypted using GPG/PGP. Other forms of Internet communication will not be used except for messages containing no proprietary or sensitive content (e.g., to schedule a phone call). In particular, details of an attack or information about

vulnerabilities will ***never*** be transmitted by any form of email or Internet communication, whether encrypted or not.

Team members may use the telephone to communicate with other project participants. Communication of proprietary or sensitive content may occur over the telephone.

Finally, please avoid discussing proprietary or confidential information in public spaces where others might potentially overhear.

5. Personal Laptops, PDAs, and Such

Personal laptops, PDAs, and other devices (called "personal devices" here) may be brought into the secure facility and used. They are to be treated as green devices. In particular:

1. Neither proprietary nor sensitive information may be installed on any personal device, unless:
   (a) It is encrypted using GPG/PGP encryption; and
   (b) It is on the personal device only for the purposes of emailing to another team or team member.
2. Personal devices may be connected to the green network. They may not be connected to the red network, nor may they be connected to any red system.
3. Transferring data or software from a personal laptop to a red machine will proceed as for a transfer from a green PC to a red PC, as described above.

6. Project End

At the end of the project, CDs of the reports, data, and all other information from the study shall be created. The CDs will be given to the Secretary of State's office for their use. Then, all removable media shall either be shredded (CDs, DVDs, etc.) or securely wiped (removable drives, memory sticks, etc.). All systems, whether red or green, shall be securely wiped.

7. References

- "Scope of Work", Exhibit A, Agreement No. 06158101 (May 2007).