Security Plan for Source Code Review Teams

David Wagner, Principal Investigator, University of California, Berkeley

1. Compliance with this security plan is mandatory for all participants in the project with access to voting system source code.

Secure facilities

2. Each site will have a room or rooms where the work is to be performed. Access to the room will be limited to project participants. The room will be kept locked at all times.

3. The facility will have a safe or other security container inside the room. The team leader will be responsible for sharing the combination to the safe with team members. The combination to the safe will be made known only to authorized source code reviewers or Principal Investigators, and only after they have signed the relevant Confidentiality Agreement, the Acknowledgement of Statement of Work, and the Security Plan.

4. The room will contain dedicated desktop PCs which may be used for processing source code. Source code will not be installed on any other machines. To prevent confusion, there will be no other desktop PCs in the room.

5. Each PC will have an external hard disk (e.g., a USB or Firewire hard disk). Team members will exercise reasonable caution to ensure that all source code and related information is installed and stored only on the external hard disk, not on the PC's internal hard drive.

Labeling

6. The facility will use strict "air-gap" security and military-style red-black separation.

7. The room will contain a supply of brightly colored labels to be available in the room, e.g., red labels. Any machine or device or storage media that contains or is involved in processing source code will be clearly labeled red. Any network cable that is attached to a red device will be clearly labeled red on both ends. Any device that is connected to a red network cable will be clearly labeled red. All desktop PCs in the room will be labeled red.

8. The red network must be contained entirely within the physical security perimeter of the room. No machine or device in the room will be plugged into any network cable that extends outside the room at any time. No red computer will have Internet access or wireless capability at any time.

9. External hard disks and removable storage media (e.g., USB dongles, CD-Rs, DVD-Rs) will be labeled red once source code has been installed on them. CD-

Rs or DVD-Rs may be marked to identify them as Confidential in some other way (e.g., using a red pen).

10. Once a machine or storage device has been labeled red, it will remain labeled red. Nothing that is labeled red may be removed from the secure room. Proprietary documents, print-outs, and other paper documents containing proprietary or sensitive material will remain in the secure room and will not be removed from it. These items should be shredded when no longer needed, or at the end of the project at the latest.

11. Exception: For purposes of enabling off-site backups of working notes, draft reports, and other data, team leaders and Principal Investigators may authorize the creation of an encrypted backup of project files.
Team leaders will exercise reasonable caution to avoid including vendor source code in this backup. The data will be encrypted using a cryptographic-strength program, such as GPG/PGP, with a high-security key or passphrase held closely by the team leader or a Principal Investigator.
It will then be written in encrypted form onto a CD-R or DVD-R, which will be labeled as confidential and may then be removed from the premises and stored at a secure facility separately from the cryptographic key.
Backup discs will be destroyed upon completion of the review of that voting system.

Intranet

11. Team members can use any network applications they like on the internal red network, including but not limited to email, chat, Wiki, shared document repositories, etc.

Clean-desk policy

12. Before leaving the facility to go home for the day, team members will disconnect their external hard disks and place it, along with any proprietary documents, working notes, removable storage media, etc., into the safe.

13. The last person to leave the room will check that all external hard disks, removable storage media, proprietary documents, and working notes from source code reviewers have been placed into the safe. The last person to leave will check on their way out that the safe is locked and that the door to the room is locked.

Personal laptops

14. Team members may bring laptops into the facility, subject to the following restrictions.

15. Vendor source code will never be installed on laptops.

16. Laptops may be connected to the Internet via an external wireless network while they are in the room, but they may not be networked to any other machine.

17. Team members may use removable storage media (e.g., CD-Rs, DVD-Rs, USB dongles) to transfer files from laptops to red PCs in a unidirectional fashion. Read-only media are preferred for this purpose. However, files shall not be transferred from red PCs to laptops or to any other
(non-red) machine.

Communication

18. 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 confidential content (e.g., to schedule a phone call).
Source code will never be transmitted by any form of email or Internet communication, whether encrypted or unencrypted.

19. Team members may use telephone to communicate with other project participants.

20. Team members will avoid discussing proprietary or confidential information in public spaces where others might potentially overhear.

Completion of the project

21. Upon completion of this project, a team leader or Principal Investigator will perform or witness the secure erasure of all storage media, devices, and PCs labeled red, before they are removed from the room (e.g., to ship them back to the Secretary of State). The secure erase tool should use a low-level overwrite of the entire partition.

22. After securely erasing red USB flash drives, CD-Rs, and DVD-Rs, they should be physically destroyed or damaged to prevent inadvertent reuse.