Concerns in the use of ***Endpoint Agent*** Security Tools

Deke Kassabian
Internet2 SALSA Group
and the University of Pennsylvania

October 14, 2008

The Issue

- Some security tools require users to install an “agent,” a small software component that runs on the users endpoint.
- Examples include:
  - Some asset management tools
  - Some tools that look for personally identifiable information (PII)
  - Some virus protection tools
  - Some network access control tools
- Agent software runs on a laptop, desktop or handheld with the privileges of the primary user, or with full administrator privileges.
- The agent coordinates with some central console software.
- This talk explores security and privacy concerns related to deployment of such agent-based tools.

Goal of this Discussion

- Organizations are encouraged to consider the scope and implications of deployment very carefully.
- When considering agent-based security solutions, it is important to understand their capabilities.
- Ironically, those software agents with the greatest capabilities could raise the greatest concerns.
- In cases where the agent has very extensive access to user data, there could be a significant risk to both privacy and security.

Configuration, or Content?

- Is the real goal about testing system *configuration*, or about system *contents*?
- The difference may be important as you consider technical approach and suitability of tools.
- Configuration vulnerabilities can probably be found in less intrusive ways than most techniques used to audit system contents.
- If it really is about content, then there may be some questions about data administration.

Data Administration?

- Who is responsible for the data involved?
- Some organizations have technical staff with a “data owner” or “data administrator” role.
- These people see to the responsible handling of certain datasets, often from a security and limited distribution standpoint.
- Do those who deploy the agent software and those responsible for sensitive data sets have the same goals and clearance.

Unique Community

- A corporate IT setting may have a different community.
- Users/employees may be predominantly using company-supplied computing equipment.
- Common ground: Protection of local networks and other local IT assets.
- But, colleges and universities may have different relationships with their user communities than in many corporate IT environments.
  - Users may be more “transient”
  - Users may be using their computing equipment
  - Users may have different expectations about privacy
- Many of our universities and colleges have a more diverse community of users with a range of relationships to the organization.

Community – Staff

- Non-faculty employees of the university
- Typically have a traditional employment arrangement, including use of employer-supplied computing equipment.
- This community may be the simplest to consider for the purposes of this discussion.
- Their use of an employer provided computer is likely governed by the terms of their employment, and agent-based tools may be very appropriate.

Community - Faculty

- Members of the faculty may have computing equipment acquired in a wide variety of ways.
- Some may have computers supplied by the university.
- Some may be using their own personally purchased computers, or computers that are part of some other professional relationship they have with another employer.
- Others may have computers purchased using grant dollars.
- In some of these cases, the faculty member may be reluctant to install software whose value they question and which may in fact threaten to compromise their privacy or agreements with other entities who may have provided the computing equipment in question.

Community – Visiting Scholars

- Like faculty, these users may have computing equipment acquired in a wide variety of ways.
- Few have computers supplied by the university.
- They may be more than reluctant to install software whose value they question – they may be prohibited by the terms of use of the supplier of their computer.
- They may also be unable given the level of permissions with which they operate on the computer.

Community – Resident Students

- Resident students often arrive on campus with personally owned computers.
  - They use campus networks full time, at all hours of the day.
  - In some ways, they are like a home user and we are like their ISP.
- They may be reluctant to install software whose value they question and which could threaten to compromise privacy.
- They may or may not be able to meet explicit goals of end user agreements such as appropriate use without these tools.

Community –
Part time / Professional Students

- May have personally owned computers, or laptops supplied by employers.
- In the latter case, they may be prohibited from installing agents by their employer’s terms of use.
- In fact, they may be unable given the level of permissions they have on the computer.

Community – Conference Attendees

- These users may have the “weakest” relationship with our colleges and universities.
- They are briefly on campus, and have what they believe to be reasonable expectations for network access.
- Do we ask them to install agents for the period of their visit?
- Do we have a way to assure them that they are fully removed when they leave our campus?

My Direct Experience

- Recently, I looked at a few Network Access Control (NAC) solutions.
- One established vendor in this space boasted about the capabilities of their agent software.
- Their NAC system could query agents on laptops and make access decisions based on fine detail about applications and data files present on the end-station, about processes currently running, and more.
- As a quick example, they showed an easy to create rule that allowed detection of a Windows computer running “Notepad”.
- They went on to describe their extensive capabilities in recognizing p2p file sharing tools installed on end-stations.
- At what point do these capabilities become “spyware?”

A Risk of "over reach"?

- If we do deploy "spyware" on endstations on our network, do we risk being asked to use these extensive capabilities to search for
  - Particular applications, or media files whose names suggest material that may be copyright protected?
  - Data that might indicate plagiarism?
- Will some ask for these capabilities to be used in large "sweeps?"   For example, do the words "plastic" and "explosive" appear close together in any files on any user computers?

Rich new attack surface

- Aside from the privacy risks, there are associated security risks.
- Throughout the Internet, attacks are increasingly being aimed at security products.
- Each such deployed tool can be an attractive target.
- In a case of “too much of a good thing,” proliferation of such tools may increase potential exposure rather than reducing it.

Powerful Tools, Powerful Concerns

- A basic review of some of the available agent-based solutions coming into common use shows that many are powerful tools that provide important information to IT staff, but could as easily provide a wealth of valuable information to an attacker.
- In some cases, the contents of all files on the computer in question are searched as a part of the regular operation of the tool. As just one example, such a capability mis-applied could prove very valuable to an identity thief.

Conclusions

- Agent-based tools can often provide useful functionality that helps to meet security, data protection, and asset management goals.
- Decision-makers should carefully consider the potential risks to both security and privacy associated with such deployments.
- Each tool will have associated benefits and risks, and in all cases care should be taken in the application of such tools.
  1. We believe that not every tool is suitable for every environment.
  2. In some cases a given tool may be more appropriate for certain portions of a user community, less appropriate for others.
  3. When simpler and less intrusive techniques are available, they should be strongly considered.

Discussion questions

- Should it be a goal to use the **least intrusive means** to achieve a necessary goal? If so, are agents the least intrusive means, or could passive monitoring get us close enough?
- Are agents available for **all relevant systems**, or just for a few "mainstream" operating systems? Will that discourage diversity, experimentation and selection of the best system (rather than the "best system that we support"?)
- In cases where agents are installed, **will users be fully informed** about what the software does and why it does it? Is consent required, and if so, what is to be done with those who withhold consent?

Discussion questions

- Are these sorts of systems **consistent with contracts** that have been negotiated with organized labor? Some such contracts may limit or forbid workplace monitoring of union member's computers.
- What is the **nature of the communications between the agent and the console** or system with which it communicates? Could someone hijack that reporting channel to gain access to confidential information?
- Can the **agent be made to only report in university-relevant circumstances**? (e.g., only if connected to a university network connection, but not when the machine is connected via a private cable modem or DSL connection?)

Discussion questions

- What **other affects will the agent have when operating on other networks?** Could another network's policy (inadvertently) prevent connection? Does the agent allow for multiple configurations simultaneously, based on network location (e.g., in the event that both organizations use the same agent with different configurations)?

- What if there is a **conflict over required agents** mandated for different roles? For example, one venue (such as a university) may mandate a particular agent while another venue (such as the student's workplace) may mandate another. What if they cannot co-exist?

- If the agent based software discovers an issue, **is the institution always ready to correct the issue** now that you've been made aware? If not, there may be risk to going out and “looking for trouble.”

Discussion questions

- If potential criminal activity is discovered, **is evidence discovered through this mechanism legally-admissible**, or would it be considered excludable as the product of a warrantless search that also lacks probable cause? Would the evidence so-collected survive evidentiary chain-of-custody challenges?
- If a **vulnerability is discovered in the agents themselves**, how would it be mitigated? Through a campus-wide upgrade or uninstall? If those capabilities exist, how can we be sure they won't be perverted/misused to install malware or to uninstall the agent at a strategic time without notice to central IT?

Thank you!

Deke Kassabian
Internet2 SALSA Group
and the University of Pennsylvania
October 14, 2008