Sharing a Little Too Much

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Recently I was invited to a business meeting using a conference call to discuss a consulting gig with a potential client.

I suggested we use Skype< http://beta.skype.com/en/ >, which allows us to hear and see each other and also share screens. However, the company sponsoring the meeting uses a different system with similar functions. The software, from a major vendor, provides a virtual meeting room with sections on the screen corresponding to the list of host(s), presenter(s), participants and teleconference information. The main section allows easy screen-sharing.

The first observation that alerted me to security issues with the software was that there was no restriction on who could enter the meeting room. Given a URL in the form < https://client-company.tool-provider.com/numerical-code/ownername >, the login screen includes two options:

- Enter as a Guest, which asks only for an unauthenticated identifier;
- Enter with your login and password ("required for hosts, recommended for registered users").

There are no restrictions at all on who can use the URL once it is known. Any guest given the URL can resume use of the virtual meeting room at any time and cannot be blocked.

After login, the tool provides teleconference information; in the meeting to which I was invited, there was a toll-free telephone number for linking in by phone. The panel showed the numerical code number used for joining the call; unfortunately, it also showed the code number for the moderator. Thus anyone accessing the panel before anyone else entered that moderator code could take control of the conference call.

The worst aspect of the virtual conference room was that the instant messaging function ("Chat") showed a conversation from several days before between two employees. My contact at the sponsoring company confirmed that there is no automatic method for clearing the chat panel at the end of a conference call. Thus I was startled to see informal comments still on the screen in plain view. Luckily, there was nothing inappropriate or confidential about the text; however, my security-conscious brain instantly imagined a situation where the same meeting space might be used for internal communication – and then made visible to others with no business having access to the internal communications. What if there had been an instant-message discussion of the client on a Friday and that same client logged in on the following Monday? Are all the users of the chat function aware that their texts could be available to anyone logging in at any time?

I discussed the security issues in this product with a helpful member of the product's technical support team.

- There is an option to specify users for a meeting; a popup for host asks for approval.
- There is a feature that allows the organizer to have the system register a user's e-mail address and a specific password created by the host.

- It is possible for the host to provide identical passwords for all participants when sending them password-reset links.
- Once logged in to the system the first time, the registered participants *must* change their passwords themselves.
- The host has no feature available to schedule termination of a meeting.
- The host can delete a specific meeting room at any time.
- The host can create a new meeting room for each meeting.

In discussion with the technical-support specialist, I made the following suggestions to improve the security of the product:

- **Require authentication:** having an option for security-naïve users that lets anyone log in as a guest without a password is unacceptable. I demonstrated the inadequacy of such a system by logging in successfully as Mickey Mouse. Users who don't routinely think about information security may simply not realize the danger of relying on security by obscurity (knowing the URL for the meeting room) as the only barrier to unauthorized access.
- **Virtual meeting rooms with limited lifespan:** there *should* be a feature allowing a virtual conference to have a specified termination date and time so that nothing from a specific meeting persists beyond the organizer's preference for termination. If I were designing the human interface, I'd make that a default specification (e.g., all meeting rooms are to be deleted after a specified time) – perhaps a time configured by a master administrator so that all meeting rooms run by employees must conform to the organization's standard.
- **Automatic deletion of chat logs:** when a host is about to log off, I would have a *default* popup message warning them that all chat messages will be deleted unless (s)he countermands this process. The notion that possibly confidential internal discussions or discussions with specific clients might be visible to others sends chills up my back.

At the user level, I would not permit such tools to be used in an organization without careful vetting by the security team. No conferencing tool (or for that matter, no software at all) should be in use by employees without approval of the security or information technology group. The responsible experts should formulate specific policies and procedures for using the new tool safely. No user should be authorized to use a tool with potential risks without adequate training.

This experience reaffirms my long-held belief that protecting confidentiality in electronic systems is not a game for amateurs. Every organization designing any product should be integrating security professionals into their development team to identify vulnerabilities and illustrate the range of exploits. Designers need to make security thinking part of their routine, not just something thrown into the mix as an afterthought. Organizations need to take control of their software environment to prevent inadvertent security breaches by their employees.

Sharing is great, provided we know what we're sharing – and with whom.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *