Virus-checking Internet Mail

Paul Ducklin, Matthew Brown

Part # tr00088g/960529

There is currently a lot of interest in products able to perform virus checking at Internet gateways. Some people see this as the "way forward" to allowing safe Internet access to employees inside their organisation.

Virus checking gateway

Conceptually, a virus-checking gateway is simple: anything that arrives at the gateway from the outside is submitted to the virus checker first. Only items which are considered clean by the virus checker are allowed to pass through the gateway to the inside.

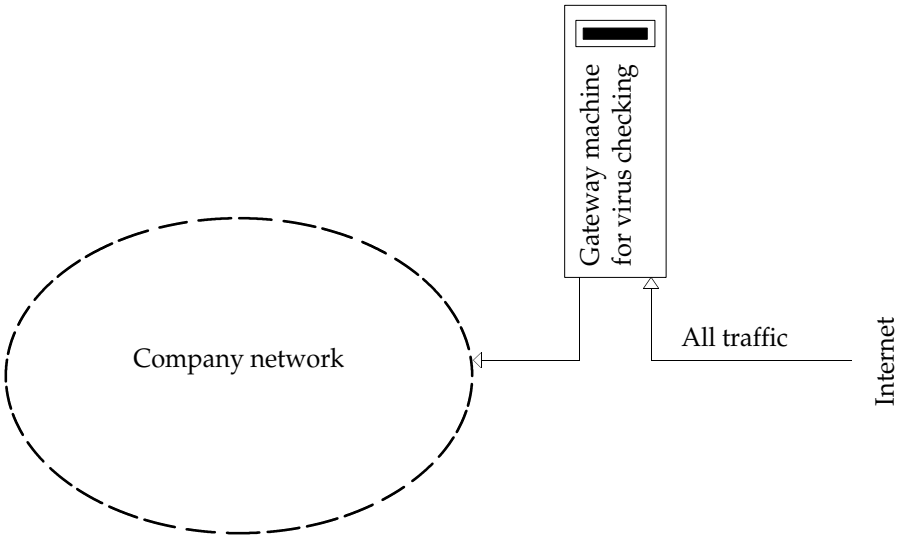
Implementing a gateway checker is non-trivial, however. A typical Internet gateway will handle hundreds of different types of message, with individual messages potentially packaged in hundreds more application-specific formats. Gateway checkers must make simplifying assumptions which allow them to detect Internet objects in certain recognisable formats, and to grab those for checking.

Everything else must be allowed through unchecked if the Internet gateway concerned is to continue functioning correctly. Typically, then, gateway checkers can only look for viruses in some of the possible Internet vehicles in which they might travel.

Checking incoming mail

Once the checker has isolated the subset of Internet objects it is prepared to take responsibility for, it must then break down those objects into their constituent parts. Then it must decide which, if any, require further attention. For example, a virus checking gateway might know about Internet mail. It then pulls all mail messages out of the incoming stream of Internet traffic, and submits them to scrutiny. The checker then needs to work out if there are any attachments in the incoming messages, and if so, how to deal with them.

Unfortunately, there are numerous "standards" for Internet mail attachments, each with its own way of packaging, compressing and encoding files inside the attachment. Most Internet encoding schemes convert binary files into some form of printable (though not readable) textual form, which helps ensure they will pass unaltered through any



Automatic virus checking of incoming mail

gateways they reach. Since this form of encoding typically makes files larger, they are often automatically compressed first to save space. Once again, there are numerous compression methods around.

Clearly, **gateway checkers can only vet attachments that are compressed and encoded using schemes they know about**. Non-standard attachments are easy to create, maliciously or otherwise, and present a problem to the gateway checker. How do you differentiate between a plain, textual email and a textually-encoded binary file that the recipient can convert via some automatic process into a potential virus carrier?

Secured email

In the case of Internet mail, there is another more serious problem faced by anti-viral gateways: proper security. Internet communications are inherently insecure. Email, for instance, can be accessed and examined on every gateway it passes through. Increasingly, therefore, companies are turning to strong encryption systems (such as PGP, and Sophos' own PUBLIC) to provide a means for using insecure networks for the transmission of confidential information.

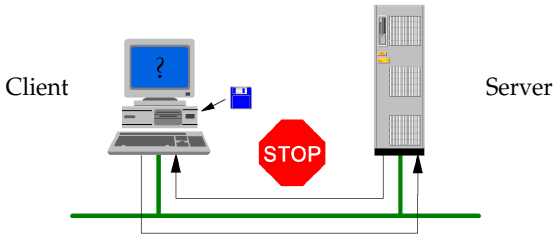
Encrypted messages remain meaningless until they are decrypted, hopefully by the legitimate recipient, and cannot thus be snooped upon at gateways - either by human attackers, or by virus checkers.

There are thus several levels of complexity and uncertainty in gateway-based virus checking. Gateway checkers typically define a subset of the problem, and cater for that. Then, they may cover only some of the possible options within the original problem subset. Finally, there are modes of use which, by design, they cannot handle.

InterCheck approach

Sophos' InterCheck is designed with rather different functionality in mind. InterCheck works transparently at the point where potential sources of infection actually appear. Instead of needing an FTP gateway checker, an email gateway checker, a floppy-disc-in-the-suitcase checker and a magazine-cover-CD gateway, InterCheck vets files and diskettes as users tries to introduce them to their systems.

Is the disk infected?



Have it checked by the server...

When a previously-unseen floppy is inserted, for example, InterCheck interrogates the boot sector and makes sure it is clean. When an email attachment is detached or launched, InterCheck interrogates it before allowing it to be used. Since InterCheck sees the results of any detachment, dearchiving, decryption, decompression or installation utility, it effectively operates independently of the way in which the object it is examining was introduced.