



Covert Channels: Data Theft

Anticipate the inevitable

Jürgen Pabel, CISSP

The first installment, "Covert Channels: Connectivity", documents some of today's more popular methods to circumvent access controls in networks. This time around, the focus is on covert channels and data theft. It would be fairly easy to argue that data theft is only a result of control circumvention. However, covert channels, that facilitate data theft don't have to provide the attributes which are essential for responsive communication paths: low latency and high throughput.

Even a system with high latency and small throughput provides perfect opportunity for covert channels - take the Email system for example: if someone wanted to send a document to an outside cooperative, it would be trivial to hide the entire document within a single, inconspicuous looking message. A simple transformation into BASE64 format would be necessary to prepare the data in a format that can then be inserted in the message in a header-field; these fields are currently neither inspected nor filtered by any of the usual mail security products. Doing so would probably not be very effective, the nature of a covert channel is that it integrates the content into an existing data record or path. Although this subversion should in most cases be detectable through human analysis, it might not be a feasible task for an automatic process. The problem with covert channels is that anything can provide the transport: even the sheer fact that a specific event occurred might be a covert message: leaving the light on in one's office at night may just be signal that an insider agreed upon with their adversaries. Statistical analysis is probably the most suitable automatic tool available for detecting covert channels; however, depending on the competence and determination of the data thieves, it may very well not even be automatically detectable then.

For most environments, data theft doesn't even require any ingenuity to remain undetected - if a file is uploaded to a web server through a SSL secured connection, no one will ever be able to prove that this did indeed happen. Once again, HTTPS is at the root of all evil... well, not all evil - but it is a very problematic topic. In the first installment I mentioned SSL-Proxies, in that context they weren't further detailed as they don't provide a realistic solution to the problem; however, in the context of data theft, SSL-Proxies are a valuable tool. Essentially, a SSL-Proxy works just like a normal HTTP-Proxy, only HTTPS connections are handled differently: instead of routing the connection request to the target server, the SSL-Proxy assumes the role of



the target server. The client software would usually notice and report this impersonation, but in the case of the SSL-Proxy it doesn't: one step in the SSL-Proxy deployment process is the installation of a custom certificate on all proxy clients. Only because of this certificate is the SSL-Proxy able to complete the SSL negotiation in a manner which raises no alerts on the client.

So, what is the solution for the threat that covert channels represent? -Not technology, I can assure you of that: as shown in the first installment, current technology has many security issues that, if anything, provide opportunities for efficient covert channels. Technology is only a tool, and organizations must wisely decide about which responsibilities they want to entrust technology with.

Organizational processes and policies are of utmost importance in establishing and maintaining acceptable behavior and action. Social competence is another key aspect: by knowing and understanding employees, it should become evident whether individuals are in fact dedicating themselves entirely to the benefit of the company.