2006-09
How can I show I am me in email?

Introduction:
Authentication is fundamental to effective communication between a CISO and those within an enterprise. So naturally, when a CISO gave me a call and asked what else they could do about this problem, I wrote it up for the rest of you to enjoy.

I need to warn them, but...
A warning is called for when a rapidly spreading virus starts to show up on an enterprise network and the defenses cannot yet defend against it. Such an example was the Microsoft Excel virus that showed up a few months ago. Naturally, the warning had to go out to all enterprise users so they could prevent accidental execution of the virus and infection of themselves and others. And naturally, the warning went out with a PGP signature on it – to prove that it was sent by the CISO. But did it actually prove anything to anyone? Of course the answer is likely not.

The problem is that anyone could send an email claiming to be from the CISO and unless the workers have a way to tell the difference, such a alert could be harmful. OF course the legitimate CISO is the legitimate CISO so there is not harm in them claiming they are they, but how do they train the workers to do what they say to do and not what a forger might say to do?

Why isn't a PGP signature good enough?
Two of the most common assumptions people make when using digital signatures or similar technology are that:

(1) the recipient will be able to use it and
(2) if used it gives meaningful information.

Of course each of these can be true, but both of these are rarely true. And in an enterprise with many thousands of workers, using digital signatures without a well staged deployment, maintenance, and operations plan, is likely to produce neither. Sure – some people will have PGP or GPG installed, some will even know how to use it, some will have it integrated into their email clients, but most will not. And even if the entire enterprise has proper installations and training on how to use the system, a forgery using a similar name, a break-in to the CISO's system, or other similar events could cause the signature to produce a false sense of security. If the CISO cannot securely communicate vital information to the workers in an enterprise, how can we expect anyone else to?

The three steps to authenticity:
At the heart of the matter, three issues show up:

(1) How do we authenticate the individual initially?
(2) How do we authenticate them after that?
(3) How do we authenticate their messages?

The first issue has to be addressed by some higher authority; perhaps a combination of a background check and government documents is adequate to your needs, or maybe you need to have people who have personally known the individual for a lifetime and who you somehow authenticate as well.

The second issue depends on gaining some calibrated parameters of the individual and using them to assure yourself who they are at a later time. Something they have, know, or are is the typical list – add something they can do if you like. Forgery is always a problem as is alteration of the calibrated copy of the data.

The third issue is the really tough one because it depends on the rest of the chain. If the first or second fail, the third fails as well. And even if the first and second work, the third is potentially problematic. The typical solution is a training and awareness process that introduces the CISO to the population of the enterprise and builds up sets of rules and procedures. Two person control over a Web site combined with an email is a really good way to do this. The CISO posts the email to everyone, complete with digital signature, and the Web master puts the notice on the internal Web site based on a telephone call or personal meeting with the CISO. The CISO does not put the URL in the email, but rather the workers have training that tells them where to look and advises against clicking on any links in the email. The process takes another minute or two to create, and the workers get independent verification that they are required to apply per training.

Conclusions:
This solution is not ideal. A skilled attacker might be able to isolate some systems and create forgeries that make a false posting look real. A secure pre-deployed technology solution might do a bit better – or not. But this solution has some features worthy of your consideration:

(1) It is essentially free to implement if you already have email and an internal security Web site
(2) It can be put in place today with no notice and trained over time to increase effectiveness.
(3) It works pretty well – better than many of the more expensive alternatives.

Better – Faster – Cheaper – All three!

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 51, section 2.6.2.4 we present:

"Phony job interviews (employee)"

> *"Some folks who want to get information on a company will arrange to get a job interview by applying for a job with a fake resume. In the interview process they will ask questions and get tours of facilities that they can then exploit for the information on what is where, to plant a surveillance device, or to leave an explosive if sabotage or extortion is their goal."*

Most such cases go unreported because they are undetected. In some of our protection posture assessments we have tried this technique and we know it doesn't work unless you have time (at least weeks) and multiple personality profiles (the odds of getting an interview are not that high). The best defense against it we have ever seen was in an interview with the CIA where an interviewee was walked down a hallway and shown the outside of a large number of unlabeled doors and told that these were the sorts of project rooms they would be working in. They were not shown the inside of any room, of course, only an unmarked hallway in a building and a meeting room where they were interviewed.

Chet's Corner

When the winter comes many folks head south. For me it's Florida. Florida combines many of the best and worst that the US has to offer. It has high crime, drug dealers and importers, Hurricanes, and a voting system problem that just won't go away. But for a security guy like me, that means work, excitement, and a sense that I can make a difference. It also means that I have to coordinate lunch and learn sessions with CompUSA stores across three states to keep our weekly security lunch program going, so be patient with me while I meet another 50 people and coordinate more stores into our program.

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's workshops:

One of the favorite things we like to do is share our knowledge with others. This comes in three forms:

> (1) Educational courses at the graduate level through Universities.
> (2) Awareness program development where we help enterprises and add select content.
> (3) Workshops where we meet specific needs while exchanging knowledge.

In a workshop, we send one or two folks out for two or three days to meet with key decision-makers. In these meetings, we present content and facilitate a series of decisions ranging from company stance on issues to specifics of structure and architecture. The group process we use helps to build consensus around a these decisions and generates authoritative agreement on key decisions that have to be made. It also educates the group and produces a commonly agreed set of facts and assumptions.

> In one recent workshop, we helped identify a series of issues that resulted in major changes in process at a large enterprise. Over a period of about a year, they turned their processes around and were able to address security more effectively and for less money.

While the new knowledge gained by the individuals helps reduce friction and increase clarity surrounding key decisions, the decision-making process itself is the most valuable result, because it creates group behaviors that forward the goals of security and engage the members of the group and their organizations in the security process. They take ownership because they contributed to the content, and they support the activity because they helped to define it.

Mollie gets the last word in

It's back to school season here, and that means that parents and children are switching gears. Don't let your kids get into an Internet accident. Browse and blog safely. Check out: www.safekids.com