A Distributed Approach to Community and Security

Vernon Cole
11/21/09 09:06:37 AM

It all came together yesterday at 6:45 A.M. – I sat up in bed and there it was...

A one size fits all resident program, which sits on the task bar when not in active use. It is the security manager for my desktop, and keeps (or keeps track of) my Private Keys for secure access to other computers and holds all of my passwords. It knows about and is the agent for "two-factor" login authentication. It remembers how long ago I last authenticated, and how busy I have been in the interim. It is also my instant messenger, email watcher and social networking tool. It is this social aspect which is important. My community provides my security.

Before our society got quite so complex, each of us lived in a village or social group where everyone was acquainted with everyone else. We knew each others situations, and there was a leadership group – the village council, by whatever name it was known, who could be depended on to make decisions and help us get along with each other. I intend to bring back the village for a security model. Each person will have someone who knows him or her, and can vouch for his or her identity. If I forget my master pass phrase, or I loose my wallet with my pass key inside, the village council can help me with the reset or send out a notice to my trading partners to invalidate my public keys. They, as a committee, have the ability to control my electronic identity. They know my important relationships. When my daughter gets married, they will confirm her change of name and send her records to her new husband's village where that village council will connect her identity to her new family.

The village is my source for two factor identification. Let me explain... A committee of bankers has determined that there are three ways of identifying a person: by something he or she knows, such as a password, by something he or she posses, like a debit card, or by something about him or her physically, like fingerprints or a face. Any of these factors can be defeated by a determined attacker – we have all seen a movie where the bad guy shoots someone and then uses their dead eyeball to fake a retinal scan – but a combination of two factors is harder to defeat than only a single factor. If someone wants to steal my money using an ATM, they must both know my PIN, and have my debit card – two factors. If, on the other hand, they want to steal my money by electronic funds transfer they need only my pass phrase for the bank's web site. The web site uses single factor identification. My village council will know me well enough to connect my face with my pass key, and can watch me set up my first pass phrase. My bank did that when I opened a new account last week. But since my credit card company and PayPal have never seen my face, they therefore lack one of my three identity factors. My village can provide this identifying information.

Where is all of this precious information kept? Well, it depends on the information. My pass key (a "smart card" or similar device) will have some information which exists nowhere else. My laptop may have some unique information so that it can act as a pass key in some cases. Copies of some "keys" will be kept safe for me in the village server, and possibly synchronized to my desktop computer. The village server itself has its data backed up at a remote point, such as some other village or a cloud storage facility. That remote facility can be opened only by my village council – who knows when our server has been destroyed or compromised.

So we have an international web of trust, with each village holding the ultimate keys to its member's

identity. The villages must know each other, and have exchanged suitable privacy keys with some number of sister villages or regional centers. Each council is responsible for its own members.

How does this system identify a person? The village will store identifying attributes for its own members. They will probably include a person's national social identity number, such as my Tax Id or Social Security Number. They ought to have my photo and my Driver's License number. They will know my physical description and my relationships with my family members. This personal data will be kept in the secure part of the village database, to be used only if I need it. (If I am abducted by aliens, the village will have the information they need to inform the authorities of my disappearance.) Statistical information which does not identify me personally may be released by the village as part of a large data set. Directory information will be published in the village directory, unless I request that it be withheld. Some facts my be available only to members of my village or others who have a known relationship with me.

So how does the cloud of villages keep track of each individual without having a copy of his or her personal identifying information? My village will issue my own unique number for me when I register. Each village also has a unique identification number, so the combination of my village's number with my number will uniquely identify me in the world. I suggest that the village's identifying number might be the IPv6 address of its founding server. The village will know the attributes associated with my number, such as whether I am a physical person, or an alias, or a legal entity. If I am using an alias, the village will have (but not divulge) my identity as a physical person. Corporations will be linked to the identities of their officers or their public registry.

Each link between me and others will include an attribute telling to whom some information may be divulged. My banker, my lawyer, and my health care provider, for example, can get at data which the general public cannot get, and each gets access to different data. If I want to get a loan, I can provide the bank with a time-limited certificate giving its loan officer temporary permission to examine my records. My child's teacher may get information which other teachers at his school cannot. Law enforcement can get my complete data, if they present a warrant to my village council. The village council will be much happier if that warrant is electronically signed by a judge who the village computer knows, and the police officer presents his electronic pass key which shows that he is associated with a legitimate agency which has authority in my area.

Institutions can provide identities (roles) for their officers and workers. I don't really care who the loan officer is who examines my records, I just need to know that she is trusted by my bank. When a person changes roles, the link between her identity and her institution changes. For example, if she retires from the village council, the link between her identity and the village council is removed. The new council member gets a new link. The position of “council member #3” hooks to a different person, and his personal pass phrase and pass key now give him access to village business.

How do we get this started? The first villages must be started by groups of people who already know each other. Schools have a relationship with their students and student's parents. Banks with their depositors, churches with their parishioners, and neighborhoods with their citizens. As the system grows, each person's identity in one part of the system will become linked with his identity in other parts of the system, so that the resulting web can provide a very high level of trust.

Why go to all of this work? Convenience and security. A quick count of the number of passwords which I have allowed my firefox browser to remember gives 81 entries today. I have several other passwords which I commit only to memory. This computer also has three private keys for access to

secure servers, and each of these has a pass phrase to unlock the key. When I started classes at Western Governors University (an online college) I suddenly gained about ten more passwords. Each provider of learning tools required yet another password, and WGU had to email to me codes and voucher numbers to unlock each access so that I could create said password. Then, I must either write them down, or re-use one password for many sites. Neither choice is secure. If each site had a trust relationship with my school, all this would be unnecessary, and my single, secure login would work with all these agencies.

The existing system sucks... err, I mean … could use improvement. We need something simpler and more sure.