

TESTIMONY OF DR. WILLIAM HANCOCK, CISM, CISSP
Vice President, Security Practice and Strategy
Chief Security Officer
SAVVIS Communications
before the
House Committee on Government Reform, Subcommittee on Technology,
Information Policy, Intergovernmental Relations and the Census
Hearing on “Identity Related Crime, Solutions and Strategies”
September 22, 2004

Thank you Mr. Chairman. My name is Dr. William Hancock. I am Vice President of Security Practice & Strategy and Chief Security Officer of SAVVIS Communications, a large multinational telecommunications and hosting company. I am Chairman of the National Reliability and Interoperability Council (NRIC) Focus Group 2B, Cybersecurity, a federally authorized council of advisors to the Federal Communications Commission (FCC). I am also the Immediate Past Chairman of the Board of the Internet Security Alliance. I appear here today as a technical expert on the subject at hand on behalf of SAVVIS Communications.

As we have heard from U.S. government experts previously today, identity theft in cyberspace has reached epidemic proportions. Most of this is due to the relative ease in which personal identify information is available on the Internet and via other methods (such as social engineering information from helpful individuals via telephone access to help desks). I believe we can all agree that there is a major problem in identity theft that is only getting worse. Rather than re-hash how bad the problem is, I would like, instead, to focus on what we can do about the issues and pose some potential steps to solve the problems.

Who Has Access to Information is Key

The first problem to come to grips with in the area of identity management is that all information ultimately ends up in a database or data repository of some sort. Identity management is not just about what information is in a database that can be stolen and used for illicit purposes – it’s about WHO is allowed access to that information and what rights they have to manipulate it.

As an example, the concept of “what is money” has changed radically since the early 1900’s. Originally, an individual’s wealth and holdings in terms of finance were based upon collateral wealth, substantiated by precious metals, jewels, real estate or other physical holdings which had value attributed to them in some manner. These material possessions were kept in vaults or secured via legal instruments (in the case of real estate) as a method of verification of wealth. In today’s modern society, “money” is an entry in a database at a financial institution. Clearing house companies, through a systematic method of mutual

trust, “tell” each other to modify database entries that are assigned to an individual to credit or debit the database entries as financial transactions are performed.

When an individual slides a credit or debit card in the card reader at a grocery store, the bank accepting the transaction works with a credit card clearing house to authenticate the card and post the transaction debit against the card holder’s account in a database being held at another banking institution somewhere on a network. There is no physical movement of assets, like gold or jewels, between institutions. There is no signing over of real estate. The entire transaction is done via computer transactions between trusted organizations who allow each other to post credit or debit transactions, usually through a third party clearing house company to ensure that the transaction is legitimate and that funds are available in the card holder’s database account to allow the transaction to successfully proceed.

Therefore, what we think of as “money” anymore is nothing more than database manipulation of transactions between trusting institutions over network connectivity.

Encryption Alone Cannot Protect Information

A major problem with such transactions is that there are long-standing, misguided beliefs that technologies such as encryption will solve the security aspects of “trust” between the organizations which allow the transactions to happen. The reality is that an encrypted value in a database cannot be changed. Therefore, encryption is used as a secure method to get the information to the database, not to actually secure the manipulation of the value.

More specifically, we might use encryption from the source location to the destination location to “hide” personal and private data from being viewed on the networking components as the packets traverse the Internet. Ultimately, however, when the information arrives at the destination database server, it must be decrypted and then the database manipulated to change (credit or debit) the user’s financial account information based on requests that are encoded as part of the transaction. This encoded entry cannot be encrypted or the values could not be changed. This means that, ultimately, the identity level of “trust” of the originating requestor of the transaction is a problem in financial transactions.

For example in the physical world, how does the bank database at your financial institution really know that it is you, in person, presenting a credit card with a magnetic strip and running it through the card reader at the grocery store? It “believes” that the information presented to it via the transaction request is authentic, based upon the fact that a physical card is required at the originating point and the general belief that you, as a person, are the only individual who has your card in your possession and would be using that card.

Card companies go to great lengths to monitor card request activities to detect fraudulent actions. For instance, if your card is being used in one geography and then, suddenly, is used in a human-interactive way in a radically different physical place, fraud management facilities at the member financial institutions will detect this as abnormal behavior and potentially stop the card transaction, initiate a call to the card holder or a variety of other actions. All of this is well and good, but it is based on a singular premise that the authentication method used in most credit cards, even at the physical card level, can be “spoofed” or faked and the card companies must take additional actions to monitor transactions to ensure they are legitimate.

Identify Management is a Key Component To Avoid Outages

The real problems of identity management are actually much broader than those posed via individual identity theft or via credit card fraud. In fact, debilitating cyber attacks are launched daily on the Internet and private networks via a type of attack called a distributed denial of service (DDoS) attack.

In this type of attack, an attacker will use anywhere from one to several thousand “slave” (or “zombie”) PCs to send packets with forged source addresses (a technique called “spoofing”) to a destination network address for the purposes of clogging up the network connection to the address so that it cannot be used by legitimate transactions. This type of attack is successful largely because a source address on most networks is automatically assigned to a system “joining” the network without properly establishing the identity of the computer when it joins the network. Specifically, does a particular system requesting an address from a network provider actually “belong” to the organization or is it authorized to “join” the network, be assigned an address and then use the network?

The reality is that the Internet and other TCP/IP networks continue to use a protocol suite that is over 30 years old and does not contain any security or identity management capabilities. If it did, the ability to “spoof” an address would disappear and such attacks would not be possible. DDoS attacks are commonplace, debilitating and cause a wide variety of network outages on a daily basis on thousands of networks worldwide. Worse, as society becomes more dependent on e-commerce methods and techniques, the effect of a DDoS attack on businesses becomes more debilitating to the company’s bottom line. As an example, consider that power grid networks are migrating from legacy protocol suites such as DECnet and OSI to TCP/IP. As this migration happens, more and more previously private networks are eventually connected to public networks such as Internet. Also, the protocols being deployed do not have base security capabilities in them to differentiate which systems are allowed to be on a specific network and which ones are not. As a power grid network is migrated to TCP/IP, it becomes increasingly vulnerable to DDoS attacks as systems on the network do not have to provide proof-positive that they belong to the network and

can send packets to a destination via spoofing attacks. In the case of a power grid, this type of attack will not only debilitate the network, it will cause grid management systems to not be able to respond to each other in a timely fashion, which will ultimately lead to system disconnections from the grid network. This type of action means that power grids will not be able to interconnect and share load information and will cause a grid to become unstable and force a computer shutdown. This type of situation will cause a mirror of what happened in August, 2003, when the power grid in the Northeast U.S. caused a computer-controlled shutdown of connected plants.

Without basic identity management of devices that “join” a network, it is impossible to stop DDoS attacks and their ilk. It also means that simple methods to kill networks will continue to exist until management of system identities is provisioned as part of the basic protocol methodology when a system joins a network and is assigned an address to communicate with other systems on the network.

Identity Management is a Key Component for All Infrastructure

Simplistic identity schemes, such as human-readable passwords, are commonly used for network switches and routers, the core components of modern communications networks which drive all manner of connectivity from telephones to cable television. Many times, passwords are shared and easily trapped by hacker programs, which grab passwords off networks or are easily guessed due to the simplistic nature in which the passwords are created and assigned to systems, devices and applications. The use of traditional passwords for infrastructure (and, frankly, any other system or application) is akin to using a screen door on a submarine for access to/from the vessel (on the positive side, the screen door probably helps keep the fish out when submerged).

In addition, very often, database-to-database “glue” programs are initialized and set-up with a single user ID and password to allow databases to interoperate and exchange information. This is a very normal occurrence where front-end, web-based engines access legacy mainframe databases to move data between the front end user method and the backend mainframe database. These passwords are the human-readable password types and not a cryptographically sound methodology. The destination back-end database system will often list the single user ID and password of the requesting user for all database transactions, no matter how critical or secure they must be, from the front-end database engine. The result is that if anyone gets access to the front end and can bypass any control methods between the databases (and this happens relatively frequently), the default access ID and password are easily discerned and the attacker can access the backend database and data with impunity.

Conclusions and Possible Solutions

In all situations I have discussed, the basic problem of identity management of devices, applications and individuals becomes a central problem in providing a safe transaction or computing environment. Identity management of the future cannot be the simplistic password methods of the past – it will need to incorporate advanced concepts such as biometrics and cryptographically sound methods to ensure the identity of a device, application or individual is permitted to access data elements in databases and other information repositories.

So, what kind of potential solutions are available to solve these identity issues?

1. Network and application protocols need a “heavy lift” R&D and engineering effort put behind them to include security controls and methods for identity management. Inclusion of identity management techniques and methods needs to be carefully considered, tested and implemented to be successful over the long term or the problems being currently experienced will pale in comparison to what will happen longer term as U.S. society becomes more entrenched in technical methods to interoperate and exchange critical financial and personal data over networks.
2. Strong, effective individualized identity methods for U.S. citizens needs to be established in a cryptographically sound manner. Simple picture IDs issued by state governments will not suffice with interstate commerce electronic transactions; advanced concepts utilizing biometrics, cryptographically secure “smart cards” and other strong authentication methods that are securely implemented need to be completed at a national level to ensure that individuals presenting identification credentials are who they claim to be and cannot be spoofed.
3. Authentication implementation and audit rules/processes need to be established for critical infrastructures such as power networks, water processing networks, food supply, telecom supply, emergency services and other related types of network infrastructures which are becoming totally dependent on technologies to be effective.
4. Multiple methods of authentication standards need to be created and established to ensure that one authentication method, if compromised, does not cause the “house of cards” scenario and take down all other authentication methods in the process. While more technically difficult to implement, it supplies one of the base rules of computer security – defense in depth – and allows for the eventuality of any specific security component being breached by having multiple authentication methods, properly compartmented from each other.
5. Incentives need to be provided to various sectors to rapidly implement advanced authentication and identity management methods. These may

vary in composition, but might include items such as reduced legal liability if a company implements strong authentication and identity management processed and technologies on critical infrastructures or areas where privacy is paramount.

6. The U.S. government needs to lead from the front. For example, U.S. government contractual and licensing agreements need to include strong authentication and identity methods as a requirement for the purchase of products and services which provision network, database or applications connectivity. Also, there needs to be a requirement that interconnection to private sector or other public organizations (such as municipalities and state governments) possess the same if not superior authentication and identity management schemes before such connectivity is allowed.
7. There needs to be an effort to quickly compel the government and public companies to migrate away from traditional (and very weak, security-wise) human-readable and guessable passwords and access methods. The time for such controls is antiquated and are grossly insecure.
8. We need to take an international approach. For example , we could couple U.S. trade agreements with international partners to include strong authentication and identity management for all electronic transactions of any type. While this will take time, oddly enough other countries (such as Malaysia) are ahead of the U.S. in the areas of national identity management and in their government use of strong authentication methods. The U.S. cannot be left behind on this important and mission critical issue.
9. We need to migrate traditional U.S. government functionality dependency on commonly accessible information, such as Social Security numbers, and migrate to strong authentication and multi-level identity management schemes to protect citizen privacy and confidentiality of information.
10. Any legislative or regulatory efforts in the area of identity management need to be on a larger scale than just the protection of a password, an individual's private information or a financial transaction. Identity management is a key component of a multi-level security strategy to properly protect critical infrastructures at many different control points. Identity of devices, applications, individuals and the mixing/matching of all comprise a wide range of identity management challenges that must be solved to ensure that the U.S. economy stays safe and secure.

Thank you, Mr. Chairman, for the opportunity to testify today. I will now be happy to take any questions.