LIBERTY
ALLIANCE
PROJECT

Liberty Alliance Glossary: Identity Theft Primer

December 5, 2005

Appendix A – Glossary of Attack Vectors

Dumpster Diving: Personal information found in the trash may be used to access accounts and perform account maintenance.

Evil Twins: An “evil twin” is a wireless network that pretends to offer trustworthy Wi-Fi connections like the kind commonly found a local coffee houses, airports and hotels, but .is actually a ruse designed to steal the consumer’s passwords and credit card numbers.

Family Members, Friends and Co-workers: It is estimated that one-fourth to one-half of all identity theft is committed by family members who may know authentication information.

False ATM Card Readers: Fake ATM machines located in public places capture card numbers and PINs without dispensing money.

Hacking: This attack vector involves obtaining unapproved access into an organization’s computer systems, databases or intranet to steal confidential information. Financial services organizations, schools, large retailers and payment processors are frequent targets.

Hacking wireless networks: While wireless network technology is amazingly cost-effective, if it is deployed carelessly it can be staggeringly insecure. Because of a lack of enforceable standards for information security controls, it is in fact possible for a corporation to utilize this kind of technology insecurely, exposing critical data to anyone with the right equipment to eavesdrop on it. Worse, this equipment is starting to show up in some portable ATM machines, which means that ATM card numbers and PINs have been compromised via this means.

Insiders: One of the greatest threats to data comes from within organizations. It is estimated that a significant percentage of identity theft is committed with information stolen by employees or other participants in transactions or services. Getting access often requires little technical expertise, and high-capacity storage devices like USB thumb drives can easily accommodate the customer databases of even the largest companies, so it is extremely easy for this type of data to literally “walk out the door”.

Keyboard Loggers: A keyboard logger is a piece of software that is designed to permit an attacker to record all the keystrokes that are made on a PC keyboard and upload the information to another location. The purpose of this software is to obtain credit card numbers and user-IDs / passwords to sensitive systems. There are a number of different ways in which systems can be infected with keyloggers, but the usual ways are via e-mail-borne viruses, or by visiting compromised web sites.

Mail theft: Credit card offers, convenience checks or outgoing checks may be stolen and used fraudulently.

Pharming: This attack occurs when a consumer types in a correct Web page only to be misdirected to a fraudulent site. The criminal does this by surreptitiously changing some of the address information that Internet Service Providers store to speed up Web browsing. This attack is knowns as DNS (Domain Name Service) Poisoning or – more colorfully - pharming.

Phishing: involves using fake emails set up to look like they come from a financial organization or online retailer, to trick the consumer into providing personal information. Because many phishing attacks originate overseas, and because Web sites are quite hard to shut down immediately, the average life span of a phishing attack is over two days.

Pretexting is a particular kind of social engineering where a thief, armed with just a bit of information, calls a bank pretending to be the account holder and works their way into access.

Privileged Access: Elevated rights to access resources; generally administrator or root privileges, data base administrator privileges or the like.

Shoulder Surfing: Simply looking over someone's shoulder may yield PINs, user IDs and other confidential data.

Social Engineering: A common type of offline attack that involves exploiting human nature to gain personal information. Often an attacker gets information by simply asking for it, pretending that they are someone in authority who has a right to get it or to gain access to something.

Appendix B – Glossary of Mitigations

Access controls and user privileges: Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Access Control systems include:

- File permissions, such as create, read, edit or delete on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

Airsnarfing: A simple rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.

Anti-spyware: Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information or changing the configuration of your computer, generally without appropriately obtaining your consent. Anti-spyware is software that is designed to check a computer for spyware and other unwanted software and help remove it.

Anti-virus: Software which protects a computer from infection from viruses and worms: small, sometimes destructive, self-propagating programs usually transmitted via the Internet or discs. Infected machines can lose data and spread viruses to other computers**.**

Audit controls: A control is a protective, measurable action which enhances the probability that established objectives will be achieved, reduces the probability of exposure to undesirable events, reduces the impact of those events if they occur, and reduces the recovery time following and undesirable event.

Browser toolbar: A toolbar is a row, column or block of onscreen buttons or icons that, when clicked, activate certain functions of the program.

Encryption: Any procedure used in cryptography to convert plaintext into ciphertext in order to prevent any but the intended recipient from reading that data.

Encrypted payload: Encryption of portions of transmitted data, while leaving headers and non-confidential data as plaintext.

Honey pots/honey nets: A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. A honey net is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honey net contains one or more honey pots.

HIPS (Host Intrusion Protection Systems): A software package that loads and runs on the host system requiring protections. HIPS attempts to detect and respond to attempted intrusions into a host server or desktop/notebook system. A HIP complements firewalls or anti-virus software by thoroughly inspecting the contents of network packets arriving at the host and the behavior of the host application software or operating system.

Multi-factor authentication: Combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types:

- Secret - something the person knows
- Token - something the person has
- Biometric - something the person is.

n-tier architecture: Used to describe a solution in which a degree of separation is attained by one or many software agents between discrete components in order to facilitate processing in some manner. An example of this would be the use of middleware to more efficiently service data requests between a user and a database. It may also be referred to as a multi-tier architecture. The most widespread use of this term refers to the three-tier architecture**.**

NIDS (Network Intrusion Detection Systems): A NID system gathers and analyzes information from various areas within a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). NIDS use vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Policy and enforcement: Specifies the interplay between different entities for the purpose of delivering services while enforcing some desired application constraints and client requirements.

Real-time monitoring: Monitoring and measuring system and network developments with technology and communications systems that provide time-relevant information in an easily understood format that can be used in day-to-day decision-making.

Secure coding techniques: Techniques for software developers that span:

- Designing secure applications;
- Writing robust code that can withstand repeated attacks; and
- Testing applications for security flaws.

These include threat modeling, designing a security process, international issues, file-system issues, adding privacy to applications and performing security code reviews.

Secure configuration: Ensuring that networks and systems are compliant with local security policy and local security settings.

Separation of duties: Dividing responsibility for sensitive information that no individual acting alone can compromise the security of the network or computer system.

Server-side validation: Validating client-supplied input data at the server, as opposed to client-side validation. Server-side validation helps prevent users from bypassing validation by disabling or changing the client script.

Shredding: A means of destroying either paper records or disks by mechanically cutting the materials into a multitude of narrow strips.

SSL/TLS: SSL (Secure Sockets Layer) is the leading security protocol on the Internet. Developed by Netscape, SSL is widely used to do two things:

- Validate the identity of a Web site, and
- Create an encrypted connection for sending data.

TLS (Transport Layer Security) is a security protocol from the IETF that is based on the Secure Sockets Layer (SSL) 3.0 protocol.

Wardriving: finding and marking the locations and status of wireless networks.