CENTER FOR DEMOCRACY & TECHNOLOGY

[Common Election Security Terms]

[Air-gapped]

A network or computer is considered air-gapped when it is not accessible from the public internet. This is an extreme security measure used to isolate sensitive computers where the security risks involved with being connected to the internet outweigh the associated benefits. However, an air-gapped system can still be attacked; that is, just because it is not connected to the internet does not mean it cannot be attacked via other methods. For example, if the system still requires data to be transferred into or out of it, then the medium (USB stick, memory card, etc.) used to transfer the data may carry a malicious program. [More Info]

[Audit]

An examination of the components of an election system – paper records, electronic records, etc. – used to assess whether the result of the vote was correct. A core component of a post-election voting audit is re-tabulating some values from ballots or comparing ballot records with digital results. Generally, an election audit will require the creation and retention of a paper ballot or paper audit trail, which serves as a software-independent record of voters' intentions. An audit can occur when the election is particularly close, if there are reasons to believe it was tampered with, or, ideally, as a regular feature of the election cycle. A "risk-limiting audit" serves as a standard spot check that provides a large degree of statistical confidence that the election results are correct. [Source]

[Blockchain]

A data structure which can be used to create consensus across many mutually distrusting parties. Most commonly associated with Bitcoin, blockchains work by incentivizing parties to verify the correctness of some kind of data. In Bitcoin, all parties (or nodes) compete to produce a proof that they verified that a ledger adds up correctly. Blockchains can provide a consistent view across independent parties (if a majority of the parties are honest), but they do not by themselves ensure things like the privacy of a vote or that the vote being submitted corresponds to the voter's intent. [More Info]

[Breach]

A breach is when information stored on a computer system is unintentionally revealed publically or to some particular party. It can refer to a misconfiguration by which a database permitted access to unintended users or to an actual successful hack by an adversary. In both cases, it may not be clear who has a copy of the breached information. [More Info]

[Corruption]

Altering data to make it unusable or unreadable. An attacker who gains access to a system may not be interested in the information itself, but rather in denying access to the information for other uses. [More Info]

[Cyber attack]

An attempt to hack or otherwise disrupt a computer system or systems. Like “hack”, this is a very imprecise term. In some cases, it may be even more imprecise if it is used to refer to unsuccessful attempts to hack whereas “hack” is generally used to refer only to successes. [Source]

[Distributed Denial of Service (DDoS)]

A distributed denial of service attack is when a number of different computers are used to send a large quantity of data to a target website or system, flooding it with traffic and rendering it unreachable. The term, “distributed” comes from the fact that there are many different computers, making these attacks difficult to block easily. The phrase, “denial of service” refers to such a high volume of traffic that causes the target website or system to become unavailable to legitimate users. Generally DDoS attacks use computers or other devices that have been taken over without their owners’ knowledge. [More Info]

[Disinformation]

Sometimes generalized as “fake news”, disinformation is “false information that is deliberately created or disseminated with the express purpose to cause harm” [Source]. Disinformation is deliberately false, which distinguishes it from malinformation which is true information that is disseminated to cause harm. It is also distinct from misinformation, which is false information disseminated by accident. An example of disinformation is twitter ads claiming you could vote by text near to the 2016 election [Source]

[Exfiltration]

When an adversary has successfully gained access to a system, they may choose to copy over, that is exfiltrate, sensitive data. Just because an adversary has access to a system doesn’t mean that they necessarily will exfiltrate data. An attacker may not exfiltrate data because it does not achieve their aims, or it may increase their chances of discovery, or because the amount of data does not make it easy. This is why a data breach does not always mean that an adversary necessarily retains access to all the data that was exposed. [More Info]

[Firewall]

A firewall is either a physical device or a computer program that sits in between a computer and the broader internet and filters out unwanted connections. The firewall’s job is to efficiently filter unwanted traffic between the computer and the rest of the internet. Firewalls can be used to mitigate some kinds of DDoS attacks. [More Info]

[Hack]

Used as either as a verb or noun, or hacker (one who hacks). It can take on two different meanings depending on the context. The first meaning, less common outside of technical circles, is as a noun and refers to an

improvement or quick fix. This has lead to things like hackathons, events where people work collaboratively to prototype small technical proofs of concept. The second, more commonly used meaning, is as a verb to mean interfering with or subverting a computer system or network. Hack is an imprecise term, which can be used to refer to a wide range of activities. Using the second meaning, it is less precise to "an election was hacked", rather than say "an election was interfered with through the hacking of a particular computer system". A hacker is typically categorized based on the intent of their hacking activities: "white hat" if their intent is beneficial or "black hat" if their intent is malicious. [More Info]

[Infected]

A computer is considered to be "infected" when it has been hacked in such a way so as to follow instructions of the hacker rather than the computer's owner. An infected computer may be part of a botnet (which can be used for DDoS attacks), or it just periodically show ads or redirect a user's web browser. While it refers to a more specific action than "hacked", it also furthers the analogy of computer security as a medical analogy (i.e. the idea that one "catches" computer viruses). (There has been some concern in the academic literature about the ways in which the medical analogy can mislead lay people into bad computer security practices.) [More Info]

[Multi-factor authentication]

The use of many pieces of information (as opposed to just a password) to prove one's identity to a computer or website. Authentication is how the computer system knows that the person using it is who they say they are. Most commonly this is done by using a password, a single "factor". Because humans are generally very bad at picking hard to guess passwords, or may be tricked into entering their password information into phishing sites, passwords are increasingly insufficient alone. The most common other "factors" are 6-digit codes sent via text message or provided by an authenticator smartphone app. A more secure, but less common, factor is the security key – a physical device that resembles a USB memory stick. Using password and something like a security key or a number that was sent to your phone uses two factors, and is therefore referred to as two-factor authentication. [More Info]

[Phishing]

A phishing attack is when an attacker sends out a deceptive email with the goal of getting users to enter their login credentials into a fraudulent site or to infect the target's device with malware. Because it's relatively easy to create sites which are convincing on first glance to people who are busy or distracted, this is a relatively low-cost attack with a high probability of success. A spear-phishing attack is a phishing attack targeting a particular person. In a spear-phishing attack, the attacker researches the target and tries to personalize the phishing email to be very compelling. A simple way to combat phishing attacks is by using multi-factor authentication. [More Info]

[Probe]

A probe (or scan) of a network or computer is when another computer sends a variety of different messages to the network or computer with the goal of getting particular responses. These responses can then be used to infer information about the targeted system. While there are many benign uses for network scans (either for research, or for more effective system administration), they are also considered to be potential precursors to more serious attacks because they can give the attacker information about a network's weak points. [More Info]

[Ransomware]

Ransomware is a type of malicious computer program that encrypts files on a victim's computer so that the computer's owner cannot access them. The ransomware then holds the files hostage until the owner pays a ransom (generally by using a crypto-currency like Bitcoin, to limit the ability of the computer owner to identify the persons responsible). If the ransom is paid, the files are decrypted and the victim is able to use them again. If the ransomware is not paid within a certain amount of time, the ransomware deletes the encryption key and the files are generally permanently lost. [More Info]

[Risk-based Cybersecurity]

A framework for making decisions about managing the security risk. At a high level, it involves inventorying an organization's cyber-assets, and using that information to make decisions and prioritize actions on the basis of the organization's strategic goals. While not a progenitor of this framework, NIST has developed guidance on implementing this framework [Source]

[Secure]

Either an adjective ("a secure website") or a verb ("they secured their computer"). In both cases it refers to the quality of being immune to a particular kind of attack or attacker. A computer system cannot be generally "secure", it can only be "secure" in relation to assumptions about the capabilities of the attacker. [More Info]

[Vulnerability]

A flaw or "bug" in a computer system's construction or configuration that may be used to improperly gain access to, interfere with the functioning of, or otherwise corrupt a computer system. Vulnerabilities may be known, or unknown (so-called zero days). Vulnerabilities, like the term "secure" need to be defined in terms of a particular kind of attacker. For example, a vulnerability may be exploitable by an attacker who can observe network traffic, but not an attacker who can just send messages to the vulnerable computer. Vulnerabilities can also vary in what they will allow the attacker to do. Some vulnerabilities may permit an attacker to read data, some vulnerabilities may permit an attacker to alter data, some may just permit an attacker to disable the computer for other users. Every system or computer program has vulnerabilities and sometimes fixing one vulnerability may unintentionally create another vulnerability. [More Info]