**Handouts of Lecture 23 Professional Practices (IT)**

**Lecture Title: Cyber Crime and Cyber Attacks, online voting**

**Supervisory Control and Data Acquisition (SCADA) Systems**

Industrial processes such as chemical plants, oil and gas pipelines, and electrical power grids require constant monitoring. In the precomputer era, monitoring was done by employees who watched gauges and warning lights, turned dials, and opened and closed valves. Computers allowed the automation of centralized monitoring. In the 1980s, distributed control systems eliminated local control cabinets. Instead, networks carried information to centralized control centers. Computer monitors with color-coded fields replaced the gauges and warning lights. Initially, distributed control systems were proprietary, but customers asked for “open systems, common protocols and vendor interoperability”. They got what they wanted with the advent of supervisory control and data acquisition (SCADA) systems based on the Internet protocol. Internet-based SCADA systems are less expensive and are easier to maintain and administer than proprietary systems.

Another way to save money and time is to allow an outsider to connect with the SCADA system remotely to perform diagnostics. These advances carry with them security risks. Allowing remote diagnostics creates an opportunity for a malicious outsider to gain access. Many industrial machines contain embedded microprocessors. Industrial machines last a long time, which means many of these machines contain older microprocessors. Security patches designed to ward off malware may not be available for these microprocessors, and even if they are available, it may be impractical to install them because the processor is so slow that it cannot run the security code and keep up with its machine-control responsibilities.

**The Stuxnet worm**, launched in 2009, attacked SCADA systems running Siemens software. The worm appeared to target five industrial facilities in Iran, and it may have caused a temporary shutdown of Iran’s nuclear program by infecting computers controlling centrifuges processing uranium. There is some evidence that Israeli Defense Forces may have been responsible for unleashing the worm.

**Cyber espionage attributed to the people’s liberation army**

American computer security firm Mandiant spent nearly a decade investigating hundreds of computer security breaches in more than a dozen countries and tracing those breaches back to the organized groups responsible for them. One of these groups, labeled APT1 (for advanced persistent threat 1), was responsible for at least 141 intrusions over a seven-year period. In 2013 Mandiant released a report stating that the APT1 group was located in Shanghai, China, and most likely was Unit 61398 of the People’s Liberation Army. According to Mandiant, APT1 was responsible for stealing hundreds of terabytes of data from the 141 organizations whose computer networks it compromised. One of these organizations was Telvent Canada, which provides SCADA systems to oil, gas, and electrical power companies. After Telvent Canada became aware of the security breach, it notified its customers and cut off access to their SCADA systems from its computers in the hope of preventing a remote attack. In response to the allegations made by Mandiant, Hong Lei, a spokesman for China’s foreign ministry, stated that China enforces laws prohibiting cyber attacks. He continued, “Groundless criticism is irresponsible and unprofessional, and it will not help to solve the problem”.

**Anonymous**

Anonymous is a loosely organized international movement of hacktivists.

The profile of Anonymous was raised significantly in 2008 when it confronted the Church of Scientology. After somebody uploaded to YouTube a video interview of Tom Cruise produced by the Church of Scientology and meant to be seen only by its members, the church filed a copyright violation claim and asked YouTube to remove it. YouTube complied with the request. In response, Anonymous issued a press release stating it was going to conduct attacks on the Church of Scientology “to end the financial exploitation of its members and protect the right to free speech”. Anonymous members launched DDoS attacks on Scientology Web sites and worked to keep the Tom Cruise video available on the Internet.

In addition, more than 6,000 Anons donned Guy Fawkes masks and protested the Church of Scientology in the streets of 90 cities across North America, Europe, Australia, and New Zealand. Since then, a series of actions around the world have been attributed to Anonymous.

Here is a sampling:

Operation Payback was a series of DDoS attacks against the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), Indian company Aiplex, and the US Copyright Office. These attacks were launched in September 2009 after it was revealed that the RIAA and MPAA had contracted Aiplex to launch DDoS attacks on BitTorrent sites, including the Pirate Bay.

A few months later, the focus of Operation Payback shifted to PayPal, Visa, and MasterCard after they froze the transfer of funds from supporters of Julian Assange to the WikiLeaks organization. The Web sites of all three of these financial institutions were disrupted by DDoS attacks.

Anonymous played an active role in the Arab Spring uprisings of 2011. In Tunisia, for example, Anons launched DDoS attacks on government Web sites, offered advice to dissidents on how to conceal their identities online, and helped local activists upload videos of their protests to the Internet.

After the US Department of Justice announced action against cybervault Megaupload in January 2012, Anons launched DDoS attacks on the US Department of Justice, Universal Music Group, the RIAA, the MPAA, Broadcast Music Inc., and the FBI.

In April 2013, Anonymous launched a cyber-attack on Israeli Web sites on Holocaust Memorial Day to protest the Israeli treatment of the Palestinians.

**Online Voting**

**Motivation for Online Voting**

The 2000 presidential election was one of the closest contests in US history. Florida was the pivotal state; without Florida’s electoral votes, neither Democrat Al Gore nor Republican George W. Bush had a majority of votes in the Electoral College. After a manual recount of the votes in four heavily Democratic counties, the Florida Secretary of State declared that Bush had received 2,912,790 votes to Gore’s total of 2,912,253.

Bush’s margin of victory was incredibly small: less than 2 votes out of every 10,000 votes cast. Most of these counties used a keypunch voting machine in which voters select a candidate by using a stylus to poke out a hole in a card next to the candidate’s name. Two voting irregularities were traced to the use of these machines. The first irregularity was that sometimes the stylus doesn’t punch the hole cleanly, leaving a tiny, rectangular piece of card hanging by one or more corners. Votes with “hanging chad” are typically not counted by automatic vote tabulators. The manual recount focused on identifying ballots with hanging chad that ought to have been counted. The second irregularity was that some voters in Palm Beach County were confused by its “butterfly ballot” and mistakenly punched the hole corresponding to Reform Party candidate Pat Buchanan rather than the hole for Democratic candidate Al Gore. This confusion may have cost Al Gore the votes he needed to win Florida.

**Benefits of online voting**

Advocates of online voting say it would have numerous advantages.

Online voting would give people who ordinarily could not get to the polls the opportunity to cast a ballot from their homes.

Votes cast via the Internet could be counted much more quickly than votes cast on paper.

Electronic votes would not have any of the ambiguity associated with physical votes, such as hanging chad and erasures.

Elections conducted online would cost less money than traditional elections.

Online voting would eliminate the risk of somebody tampering with a ballot box containing physical votes. While in most elections people vote for a single candidate, other elections allow a person to vote for multiple candidates. For example, a school board may have three vacancies, and voters may be asked to vote for three candidates. It would be easy to program the voting form to prevent people from accidentally over voting—choosing too many candidates.

Sometimes a long, complicated ballot results in under voting—where a voter accidentally forgets to mark a candidate for a particular office. A Web form could be designed in multiple pages so that each page had the candidates for a single office.

Hence online voting could reduce under voting.

**Risks of online voting**

Critics of online voting have pointed to numerous risks associated with casting ballots over the Web, summarized in the following paragraphs.

Online voting is unfair because it gives an unfair advantage to those who are financially better off. It will be easier for people with computers and Internet connections at home to vote.

The same system that authenticates the voter also records the ballot. This makes it more difficult to preserve the privacy of the voter.

Online voting increases the opportunities for vote solicitation and vote selling. Suppose person X agrees to vote for candidate Y in return for getting a payment from Z. If person X votes from his personal computer, he could allow person Z to watch as he cast his vote for Y, proving that he fulfilled his end of the bargain. This is much less likely to occur at an official polling place monitored by election officials.

A Web site hosting an election is an obvious target for a DDoS attack. Unlike corporate Web sites, which have attracted the attention of teenage hackers, a national election Web site could attract the attention of foreign governments or terrorists trying to disrupt the electoral process. What happens if the Web site is unavailable and people are not able to access it before the election deadline?

If voting is done from home computers, the security of the election depends on the security of these home computers. The next few paragraphs describe ways in which the security of home computers could be compromised.

A virus could change a person’s vote without that person even suspecting what had happened. Many people have physical access to other people’s computers, giving them the opportunity to install voter-deceiving applications in the weeks leading up to the election. Alternatively, a rogue programmer or group of programmers within a software company could sneak in a vote-tampering virus. A backdoor Trojan lurking in a voter’s computer could allow a person’s vote to be observed by an outsider.

A backdoor Trojan could even allow an outsider to cast a ballot in lieu of the rightful voter.

An attacker could fool a user into thinking he was connected to the vote server when in actuality he was connected to a phony vote server controlled by the attacker. For example, the attacker could send an email telling voters to click on a link to reach the polling site. When voters did so, they would be connected to the phony voting site. The attacker could ask for the voter’s credentials, then use this information to connect to the real voter site and cast a vote for the candidate(s) desired by the attacker.

**Utilitarian analysis**

A utilitarian analysis must add up the positive and negative outcomes to determine whether allowing online voting is a good action to take.

We must consider the probability of the outcome, the value of the outcome on each affected person, and the number of people affected. Sometimes this calculation is relatively straightforward. For example, one of the benefits of online voting is that people who vote online would not have to travel to a polling place and wait in line.

Suppose online voting replaced polling places in the United States. This change would affect about 50 percent of adult Americans (the ones who actually vote). We can estimate that the average voter spends about an hour traveling to a polling place, waiting in line, and traveling back. The average annual salary in the United States is about $43,000, or about $21.00 per hour. We could compute, then, that the time savings associated with replacing polling places with online voting would be worth about $21.00 times one-half the adult population, or $10.50 for every adult. It is more difficult to come up with reasonable weights for other outcomes.

For example, a risk of online voting is that a DDoS attack may prevent legitimate voters from casting their votes before the deadline. While an election result that does not reflect the will of the voters is a great harm, the weight of this harm is reduced by three probabilities: the probability that someone would attempt a DDoS attack, the probability that a DDoS attack would be successful, and the probability that a successful DDoS attack would change the outcome of the election. Experts could have vastly different estimates of these probabilities, allowing the scales of the utilitarian evaluation to tip one way or the other.

**Kantian analysis**

A Kantian analysis of any voting system would focus on the principle that the will of each voter should be reflected in that voter’s ballot. The integrity of each ballot is paramount. For this reason, every vote should leave a paper record so that, in the event of controversy, a recount can be held to ensure the correctness of the election result.

Eliminating paper records in order to achieve the ends of saving time and money or boosting voter turnout is wrong from a Kantian perspective.

**Conclusions**

We have surveyed the potential benefits and risks of holding elections online, and we have examined the morality of online voting from a utilitarian and a Kantian point of view. Are we holding computers up to too high a standard? After all, existing voting systems are imperfect. There are two key differences, however, between existing mechanical or electromechanical systems and the proposed online system. Existing systems are highly localized. A single person may be able to corrupt the election process at a few voting places, but it is impossible to taint the election results across an entire state. A Web-based election system would make it much easier for a single malicious person to taint the process on a wide scale. The second difference is that most current systems produce a paper record of the vote. Where paper records do not exist, there is a push to make them mandatory.

When all else fails, the hard copy can be consulted to try to discern the intent of the voters. A Web-based voting system would not have paper records verified by citizens as true representations of their votes. There is already evidence of tampering in online elections. In April 2002, Vivendi Universal, a Paris media conglomerate, held an online vote of its shareholders. Hackers caused ballots of some large shareholders to be counted as abstentions. If a private election can draw the attention of a hacker, imagine how much more attractive a target a California election Web site would be!

Bruce Schneier has written, “A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in computing history”. Any election system that relies upon the security of personal computers managed by ordinary citizens will be vulnerable to electoral fraud. For this reason alone, there is a strong case to be made that a government should not allow online voting to be conducted in this way.

***Reference***

***Lecture 23 slides: Computer and network security (Cont.)***

***Gao, Y. (2012). Ethics for the Information Age by Michael J. Quinn. World Libraries, 20(1).***