

Rogue Access Point Detection Via Crowdsourcing

With all new technologies come new challenges and solutions. The ubiquitous nature of wireless networks has been a boon to convenience and connectivity. Unfortunately wireless networks are also a source for a variety of security problems. One such problem is the occurrence of rogue access points that compromise network security for both large and small organizations. Detecting and eliminating rogue access points is an ongoing and sometimes onerous task that all organizations must address.

The ever-increasing power of the Internet has created a new view toward collective problem solving called crowdsourcing. This technological and sociological phenomenon is not exactly new ("Many hands make light work"^[1]), but it is now being implemented in unique ways to solve a variety of problems. Using this technique to detect rogue access points results in higher security for a lower cost.

Rogue Access Points

One of the major concerns for wireless network security is the presence of "rogue" access points. An access point (AP) is considered a rogue when it is installed on the company network without approval. This may happen when an engineer is testing some new wireless gizmo, or when an area is temporarily setup with a wireless network for a sales meeting. In some cases a rogue access point is an overt attempt to breach network security. Anytime a rogue access point is present, the network is potentially exposed and vulnerable to the outside world.

Numerous cautionary tales are available concerning computer and network security failures. There have been several high profile cases where wireless networks were breached, resulting in the theft of millions of credit card numbers and associated account information. Even if your business does not process credit cards, a compromised network is a gateway to company financial records, privileged correspondence and intellectual property.

The theft of a single credit card number is estimated to cost a company between \$100 and \$300 for additional accounting, replacement costs and legal settlements^[2]. The loss or exposure of company secrets is an almost incalculable cost.

Detecting Rogue Access Points

Given the potential consequences of a rogue access point, what is to be done about them? Fortunately a variety of solutions exist for detecting and eliminating rogue access points. These solutions range from small, handheld instruments to large installations of network hardware and software. Unfortunately it is difficult to make a "one-size-fits-all" recommendation for the best approach to deal with rogue access points. Company size, technical expertise and available budget are all factors that must be accounted for. Some general guidelines are applicable to most situations.

When considering security it is often advisable to take a multi-layered approach. This is similar to having both seat belts and airbags in your automobile. If one system fails there is another as a backup. For a network the security layers might include restricted access, encrypted data and strong firewalls.

One excellent approach to detecting rogue access points is to combine network monitoring software and physical site surveys. The network monitoring software watches for unusual data patterns and the presence of unapproved hardware. Site surveys, or scans, monitor the radio spectrum for broadcasts from unauthorized access points.



A further discussion of network monitoring software, such as Rogue Scanner^[3], is beyond the scope of this white paper. There are numerous open source and commercial resources for this aspect of wireless network security.

Site Surveys

Site surveys are a valuable addition to all wireless network security protocols. They are able to detect situations that might be missed by wired-side network monitoring. For example, an evil twin^[4] attack from an external location is undetectable by software monitoring an internal network. Similarly, a misconfigured laptop in wireless ad hoc mode could provide a path into your wired network that appears legitimate to monitoring software.

Site surveys are most often performed by walking through a location with a handheld detection device. The detection equipment might be a laptop computer running special software, or a dedicated test instrument. When selecting site survey equipment, one should consider budget, convenience, training and required technical expertise.

As usual there is a cost for security. Site surveys have an initial setup cost and a reoccurring cost for each survey performed. It is the cost of site surveys that often prevents them from being widely or effectively implemented. This section discusses how to characterize the cost of site surveys; and the following sections present an innovative way to reduce cost while improving security.

The initial cost of a site survey can be expressed as:

$$\text{Initial Site Survey Cost} = \text{Cost of Equipment} + \text{Cost of Training} + \text{Employee Training Time}$$

The cost for equipment can range from hundreds to thousands of dollars. The cost for training can range from nothing (i.e. read the manual) to thousands of dollars for a multi-day training class. The final cost point is the time required for an employee to learn and master the equipment's operation. Unfortunately these are not onetime costs because equipment does break and employees do leave; thus requiring replacements in either case.

Each site survey has an associated cost. This reoccurring cost can be expressed as:

$$\text{Cost of One Survey} = \text{Employee Time for Survey} + \text{Employee Time for Analysis}$$

The survey time is whatever time is required to navigate the location and record observed results. Analysis time is harder to categorize. It involves comparing previous survey results and looking for unexpected changes. This can be a paper or automated process that encompasses a few data points or hundreds.

Once all of the costs for a site survey are understood, then a decision can be made about how often a site survey should be conducted. To minimize cost, site surveys could be conducted quarterly as required by the Payment Card Industry (PCI) Data Security Standard (DSS)^[5]. To maximize security, site surveys could be conducted daily.

When presented with two such extremes the answer is usually somewhere in the middle. While quarterly surveys, or scans, are the minimum requirement for PCI DSS, they do recommend that scans be performed more often. Just consider the potential expense if a security breach went undetected for three months? While daily site surveys are much more secure; the cost for a dedicated employee to perform this task might be prohibitive.

Thus the frequency of performing site surveys is a balance between risk and expense. Other factors that must be considered include what other layers of security are in place, the size of your company and the



nature of your business. For example, large companies dealing with many financial transactions better minimize risk however possible.

Therefore a company is faced with the seemingly unachievable goal of high security for a low cost. Fortunately as technology has evolved so have different methods for solving problems. One such method has recently been described as crowdsourcing. Crowdsourcing provides a unique way to solve the wireless network high security and low cost paradox.

What is Crowdsourcing?

Crowdsourcing^[6] is a recently coined term describing the act of taking a task traditionally performed by an employee and outsourcing it to an undefined, generally large group of people. This concept has been applied in a variety of situations to solve problems and complete complex tasks.

Very simply you can think of crowdsourcing as taking a large individual task and breaking it down into smaller tasks performed by many people. For example, consider one adult searching for Easter eggs in a backyard. This task would be more quickly, and enthusiastically, completed by 20 toddlers.

The idea of crowdsourcing has been around long before computers, but the Internet has greatly expanded its potential. Historical examples of crowdsourcing include Tom Sawyer painting a fence and the growing of victory gardens^[7] during World War II. Contemporary examples include software beta testing and the PlayPump^[8], a water pump/merry-go-round powered by children.

People participate in crowdsourcing for a variety of reasons. Very often there is some kind of payback for contributing. A payback might be as simple as feeling good for supporting a worthy goal. Other times the payback is that the task is fun or that there is a challenge to see who contributes the most.

How to Crowdfund Rogue AP Detection

Crowdsourcing can be readily applied to the job of performing site surveys to find rogue access points. Rather than having one employee performing site surveys with expensive equipment, arm many employees with inexpensive equipment to perform the same task. Each employee then becomes responsible for surveying the area near where they work. Since they are already familiar with their area, they can perform a "localized" survey more quickly, more frequently and more cost effectively.

The first step in crowdsourcing is to find someone to coordinate the effort. This person obviously needs to understand wireless networks and the security issues around rogue access points. Most importantly the coordinator should have good interpersonal skills and be able to motivate. Much of the success of any crowdsourcing activity is due to the motivation of the people involved.

The next step is to select the equipment for detecting rogue access points. It is important that everyone uses the same equipment in order to minimize setup, training and support costs. Trying to use existing laptops, or PDAs, will greatly increase the complexity of the effort and will ultimately be frustrating for all concerned. A common, simple-to-use, low-cost platform is best for consistency and training. By keeping the equipment costs low, more people can be involved in the program. It is far better for security to have 20 people each using a \$250 instrument than to have 1 person with a \$5000 instrument.

Next a cadre of willing participants must be assembled. Again, interested and motivated individuals best serve the task. With the right equipment, minimal technical skills are required. The key to rogue access point detection via crowdsourcing is to select a broad range of people from all physical locations within your company. For example, if you have a 10-story building you might select a few people from each floor. Ideally, assigned survey areas should significantly overlap each other. That way survey results are



not unduly compromised by vacations, business trips or sick days. Triple and quadruple overlapping survey areas are even better if the necessary people and equipment are available.

Training your “crowd” of eager participants can be accomplished in several ways. Initially you might gather them all together for, at most, an hour-long briefing on wireless network security, rogue access points and the equipment they will be using. The information presented should be kept at a high level and supplemented by handouts. The mood of the briefing can be kept light and fun by having the participants compete to answer questions or to perform tasks on the detection equipment. Prizes for the winners are always a nice touch. The “final exam” for the briefing might be a “treasure hunt” for a dummy rogue AP that has been hidden somewhere in the building. Just plugging in an access point easily creates a dummy rogue AP. As long as the AP is not connected to your network, there is no security risk. Setting the AP’s SSID to “**Dummy Rogue**” or “**Find Me**” makes it clear which AP they are searching for.

As a follow-up, the coordinator should meet with smaller groups in each of their assigned areas. That way the people surveying adjoining areas can become familiar with each other. This gives everyone a “local” contact for simple procedural or equipment questions. The coordinator should lead the group through an initial site survey to orient them with the characteristics of the access points in the area. The presence of any unexpected access points should be resolved at that time.

The coordinator needs to provide some ongoing support in order to keep the crowdsourcing effective. Questions and equipment problems must be dealt with quickly to avoid frustration and to reinforce the value of the effort. Survey logs should be reviewed to verify the frequency of surveys and to note any changes. Biweekly feedback to the participants via email, or personal contact, will keep them engaged. Share with everyone the number of surveys completed and, especially, any positive results in detecting unknown access points. To really keep interest high, sneak a dummy rogue AP onsite occasionally and present a prize to whoever detects and locates it first.

A few additional guidelines are important for rogue AP detection via crowdsourcing. If an unknown AP is detected, the program coordinator should be contacted immediately. Under no circumstances should a potential rogue AP be physically located by one of the “crowd”. This avoids potential conflicts or accusations between employees over what might be a simple error or technical glitch. Also it is vital that a network security expert evaluate the situation to determine potential exposure and necessary countermeasures. Any dummy rogue APs used for training or contests should be clearly identified as such via their SSID (e.g. “**Dummy AP**”). These then can be fully tracked to their physical location.

Some form of logging or tracking of site surveys is necessary. This provides an audit trail for understanding costs versus results for the program. If records are not kept, the program becomes invisible, misunderstood and unappreciated. An activity log also indicates which participants might need additional encouragement or might prefer to be replaced. Logging site surveys can be as simple as filling out a paper form, sending a weekly email to the coordinator or entering data into an online database/spreadsheet. The chosen method must be as simple and quick as possible in order to encourage localized surveys. A tedious or complex logging procedure discourages participants from performing more than the minimum required surveys.

Localized surveys should be conducted at least weekly. If the assigned area can be surveyed in a short amount of time (e.g. less than 15 minutes), and the paperwork is kept minimal, participants are able and willing to scan much more often. Frequent contests with prizes will encourage them to integrate surveys into their daily activities. Thus walking to a meeting or going to the copier becomes a security sweep.

Finally, no security procedure is complete without some form of testing. Besides the motivational contests, more subtle tests should be conducted to assess the effectiveness of the program. In particular, positioning an external laptop, or access point, to simulate an evil twin or man-in-the-middle attack. Tests should also be conducted with dummy rogue APs that have hidden SSIDs and ones that are operating outside regional channels (e.g. channel 13 in the US). Testing such as this keeps participants alert and identifies any adjustments needed for security policies and procedures.

After reading the preceding section you may be thinking that crowdsourcing is:

- A. Complicated
- B. Weird
- C. Not possible
- D. Silly
- E. All of the above

The next section discusses the compelling reasons why rogue AP detection via crowdsourcing is a valuable addition to any network security plan.

Why Does Crowdsourcing Make Sense?

The value of crowdsourcing network security can be evaluated from two perspectives. One view is overall cost and the other is the effectiveness of the resulting security.

The two site survey costs discussed earlier are the initial cost and the reoccurring cost of performing surveys. By accepting the premise that simple-to-use, low-cost equipment is best for crowdsourcing, we can see that a significant reduction in equipment cost and employee training counterbalances the increased number of employees involved in the program. By only conducting localized surveys, an employee spends no time traveling to and from survey sites. In addition, since the areas surveyed are much smaller, it is much easier and quicker to review the collected survey results.

Crowdsourcing does require additional employee time for establishing and coordinating the program. Exact costs are dependent upon company size, physical layout, employee wages and general overhead expenses. The extra level of security that results amply counterbalances these.

Assessing security procedures is somewhat of a dark art. It is remarkably similar to leaving a light on at night to keep elephants out of your living room. The lack of elephants proves the effectiveness of the light. Fortunately there are some concepts that can be generally accepted when considering rogue access points:

- The more site surveys the better
- Random surveys are better than scheduled ones
- Multiple surveys within an area are better than a single survey
- Having several people survey the same area offsets human error
- Smaller scan areas produce less data to consider
- Having more people involved increases security awareness

Dividing a full site survey into discrete local surveys by multiple people increases survey frequency, improves coverage and reduces human error. As each person becomes familiar with the wireless networks in their area, any changes or additions are immediately recognized and reported. Occasional testing, or contests, with a dummy rogue AP maintains alertness and incentive.

Probably the biggest affect on network security is the heightened awareness that local surveys create. Rather than assigning security to some unknown group in the basement, empowered and motivated employees are distributed throughout the company. These employees thus become local advocates for network security and a visible reminder of its importance. Thus awareness of network security spreads within the company, promoting increased vigilance and providing a deterrent to illegal activity.

Awareness → Vigilance + Deterrence



Conclusion

Crowdsourcing is an innovative approach to rogue access point detection. The irony is that it is being deployed against hackers whose tools are the result of crowdsourcing on the Internet. Crowdsourcing increases the frequency, quality and randomness of site surveys for the same or less cost of more conventional procedures. Perhaps its greatest benefit is the increased awareness of network security among a cadre of enthusiastic and motivated employees.

About JDSU

JDSU (www.jdsu.com) offers instruments, systems, software, services, and integrated solutions that help communications service providers, equipment manufacturers, and major communications users maintain their competitive advantage at each stage of the network lifecycle.

A variety of wired and wireless network testing instruments are available from JDSU including the Wi-Net Window Wireless Tester (www.jdsu.com/test_and_measurement/products/descriptions/Wi-Net).

References

1. John Heywood (English Playwright and Poet, 1497-1580)
2. Khalid Kirk, Calculating the Cost of a Security Breach, (www.thectoforum.com/article.php?prodid=664)
3. RogueScanner - Open source network based rogue access point detection, (www.paglo.com/opensource/roguescanner)
4. FR3DC3RV Online Security Blog, *Evil Twin*, (<http://fr3dc3rv.blogspot.com/2007/04/evil-twin.html>)
5. Payment Card Industry Data Security Standard, (<https://www.pcisecuritystandards.org/>)
6. Jeff Howe, Crowdsourcing: tracking the rise of the amateur, (<http://crowdsourcing.typepad.com/cs/>)
7. A History of Victory Gardening, (www.victoryseeds.com/TheVictoryGarden)
8. Roundabout PlayPump, (www.playpumps.org)