International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 1; January 2018; Page No. 1324-1325

Challenges on wireless networks

M Nandhakumar
Assistant Professor, Department of Commerce with Computer Application, AJK College of Arts and Science, Navakkarai, Coimbatore, Tamil Nadu, India

Abstract
On the perfect college campus everyone would have super-fast, reliable and secure wireless access. No matter where you went, what devices or applications you were using, or how many users were on the network, everyone would always have the perfect wireless experience. While nothing is ever perfect, college IT leaders are still going to try and deliver it, unfortunately there's a lot of challenges along the way. We first summarize the security requirements of wireless networks, including their authenticity, confidentiality, integrity, and availability issues. Next, a comprehensive overview of security attacks encountered in wireless networks is presented in view of the network protocol architecture, where the potential security threats are discussed at each protocol layer. We also provide a survey of the existing security protocols and algorithms that are adopted in the existing wireless network standards, such as the Bluetooth, Wi-Fi, WiMAX, and the long-term evolution (LTE) systems. Then, we discuss the state of the art in physical-layer security, which is an emerging technique of securing the open communications environment against eavesdropping attacks at the physical layer. Several physical-layer security techniques are reviewed and compared, including information-theoretic security, artificial-noise-aided security, security-oriented beamforming, diversity-assisted security, and physical-layer key generation approaches. Since a jammer emitting radio signals can readily interfere with the legitimate wireless users, we also introduce the family of various jamming attacks and their countermeasures, including the constant jammer, intermittent jammer, reactive jammer, adaptive jammer, and intelligent jammer. Additionally, we discuss the integration of physical-layer security into existing authentication and cryptography mechanisms for further securing wireless networks. Finally, some technical challenges which remain unresolved at the time of writing are summarized and the future trends in wireless security are discussed.

Keywords: networks, security, wireless etc.

Introduction
The first professional wireless network was developed under the brand ALOHAnet in 1969 at the University of Hawaii and became operational in June 1971. The first commercial wireless network was the WaveLAN product family, developed by NCR in 1986.

- 1991 2G cell phone network
- June 1997 802.11 "WiFi" protocol first release
- 1999 803.11 VoIP integration

What is wireless network?
A wireless network is a computer network that uses wireless data connections between network nodes. Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations [2]. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

Security
Out of all of these challenges, the one that has most college IT leaders concerned is network security.
With more and more people, devices, and applications accessing the network means more potentially sensitive data that needs to be protected.
With mobile and wireless you need to know where your users are as well as who they are and what they are doing.
This means at a bare minimum having role-based access control, and the right firewall in place. However, to there's more to proper security than just these two components, check out this recent blog post to learn more.

Cost
When was the last time you refreshed your wireless network? If you answer is more than 4 years ago, you're way overdue for an update.
The effective lifespan of today's wireless platforms is between 3 and 4 years, that's it. This is due to the pace at which devices, applications, security threats, and even our physical environments are evolving.
Beyond the 3-4 year range and it becomes challenging to maintain needed wifi performance levels and the required reliability you and your end-users have become accustomed to.
This is the reality and so is the cost associated with upgrading your wireless network. It's not cheap and figuring out how to afford everything isn't an easy task to accomplish.
Knowing what you need from an IT perspective is one thing,

getting a budget approved to actually pay for it is another.
Think about your school's Wi-Fi platform as a utility, like water or electricity. It's not a luxury to have; it's a mission-critical "utility" that enables the modern day learning and recreational environments.
There are many options out there to afford the WLAN platform your school requires every 4 years, including even financing it with monthly payments.

Capacity
Schools today are extremely dense and diverse environments; they are living and breathing systems that ebb and flow. In order to support everyone and everything IT leaders need to make sure their wireless platform was designed for capacity.
Many times we see mistakes happen that result in poor performing networks because decisions were made either because of inexperience and/or lack of knowledge.
Capacity means having context which means understanding a lot more than just coverage. Capacity addresses:

- How many devices are accessing the network
- What types of devices are there
- What are the capabilities of those devices
- What types of applications are being used
- How many users are accessing the network
- What locations on your campus are seeing the most activity

Performance Monitoring
Your campus Wi-Fi network is a dynamic, living system. You can't just set-it and forget it that will only lead to more wifi problems.
To properly maintain your network and keep it operating as it was designed to do, you have to be proactive.
Your campus Wi-Fi network should incorporate the use of real-time visibility, analytics and a network management system or NMS. This means monitoring in real-time things like:

- RF Visualization (wifi heat mapping)
- Client Status
- System Status
- Usage Analytics
- Device locations

If you can't see what's going on, there's no reliable way to know how both your wireless platform and the end-users, devices and applications it's supporting are performing.

Coverage
This is the most obvious and typically most straightforward challenge that colleges and universities have to deal with when designing their wireless networks.
Where do you need to provide wireless access? This can include: academic buildings, dorms, athletic facilities and numerous outdoor spaces.
You have to understand where your mission-critical areas on campus are and plan for them accordingly to ensure you have proper coverage.
Deploying a reliable wireless network takes a lot of skill and experience to get it right the first time and not all designs are created equal. While coverage might seem straightforward there's still a lot involved in terms of getting it right the first time around.

Density
Colleges and universities have to be able to support many different, highly dense areas, containing hundreds or even thousands of users who are all simultaneously connecting to the network.
These areas can include lecture halls, auditoriums, stadiums or any large areas that dense populations of students, faculty or guests are accessing your campus wifi network.
While this is a challenge of in itself, it's been getting exponentially harder to do with the continued expansion and growth of mobile devices and applications.
Teachers are using more technology in the classroom than ever before that need wireless access to stream data, voice and video.
Making matters more complicated are students, on average each student owns between 3-5 devices and growing.
Again, your success will come down to the quality of your WLAN design and which wireless service provider you choose to partner with.

In Closing
We can say it until the cows come home, technology is only going to get better, faster, and more diverse.
Our campus's WLAN design and entire wireless platform need to be able to adapt to new devices, applications, prevent security threats, and perform critical system updates to ensure reliability, performance and security throughout your entire campus.

Conclusion
The most important thing you can do to create a successful, campus-wide network is to start with proper planning. By establishing clearly defined goals and working with the right wireless service provider, you can guarantee your campus Wi-Fi network will support today's challenges as well as be ready to take on whatever lies ahead.

References

1. Steiner M, Tsudik G, Waidner M. Diffie-Hellman key distribution extended to group communication, in Proceedings of The 3rd ACM Conference on Computer and Communications Security, New Delhi, India, 1996.
2. Culler DE, Hong W. Wireless Sensor Networks, Communication of the ACM, 2004; 47(6):30-33.
3. Jolly G, Kuscu MC, Kokate P, Younis M. A Low-Energy Key Management Protocol for Wireless Sensor Networks, Proc. Eighth IEEE International Symposium on Computers and Communication, (ISCC 2003). 2003; 1:335-340.
4. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: Security Protocols for Sensor Networks, Wireless Networks, 2002; 8(5):521-534.
5. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless Sensor Networks: A Survey, Computer Networks, 2002; 38:393-422.