

Abstract

With the Super Bowl around the corner, nearly 70,000 attendees are preparing to travel to Santa Clara, California to watch the game at state-of-the-art Levi’s Stadium, which features the latest digital amenities for today’s wireless football fanatics. Yet these same digital amenities provide potential threats that could jeopardize the mobile phones of anyone connected to the stadium network, resulting in stolen data, a mobile botnet, or worse. This alert outlines precautions for attendees and stadium operators to take before and during this event.

Background

There are few sporting events in the world as large as the Super Bowl. With over 120 million global viewers annually and a 30-second commercial costing \$4.5 million, the Super Bowl generates a lot of excitement from media, fans and the public. Beyond just the game itself – where the National Football League (NFL) champion is crowned – the variety of multimedia technology available to fans provides a more immersive and interactive experience in recent years by playing the game inside a ‘smart’ stadium. A smart stadium is a connected stadium that offers network connectivity via WiFi, Bluetooth and a number of other digital services. Last year’s Super Bowl exceeded 6 terabytes of data consumedⁱ.

To ensure attendees have a seamless digital experience, the NFL, San Francisco 49ers, Levi’s stadium’s management, and leading wireless carriersⁱⁱ have made major investments to upgrade their infrastructures to maintain a high quality of service.

Levi’s Stadium is one of the most technologically advanced stadiums ever built. The stadium provides 12,000 network ports, 1200 access points, 1700 beacons and a DAS system. All traffic is routed via network monitoring and control systems. The stadium’s bandwidth capacity is 40gbps and provided by Comcast Business Ethernet, which is 4 times greater than the NFL’s stadium mandate that was put into place in 2015. Aruba Networks is the supplier of the Beacon and Access points in the stadium. Barcode is the supplier of the switching equipment. The stadium also has 2000 IPTV’sⁱⁱⁱ

Levi’s Stadium also promotes a mobile app, providing amenities such as ordering food to your seat, Bluetooth stadium navigation, real-time replays, and more. All of this is possible due to the 40Gbps blanket WLAN, ensuring fans can watch, eat, share & download photos and videos, and communicate their game day experience with others.

Reasons for Concern

Radware’s Emergency Response Team (ERT) experts have assessed Levi’s Stadium’s network architecture and have several concerns, listing numerous courses of action for potential hackers & exploiters - whether their agenda is political, social or financial.

Providing fans with additional connectivity is a double-edged sword. Smart stadiums can become a Bring Your Own Device (BYOD) nightmare for stadium management and wireless network operators. Open WiFi networks present one of the biggest attack vectors for network and malware-based attacks. We see two principal exploits in a scenario like the Super Bowl.

The first is targeting the user over the network. Common types of attacks to use may include:

- Compromising unsecure and vulnerable access points
- Deploying evil twins or fake cell phone towers
- Spreading malware or spam and other man-in-the-middle (MITM) attack forms
- Data mining using fake pop ups, text messages or spoofed websites
- Denial of service attack leaving fans unable to enjoy the benefits of a smart stadium

The second is compromising the stadium’s mobile app. This can be done to:

- Steal users’ data (passwords, emails, photos and other personal information)
- Acquire credit card information (for instance when ordering food via the app)
- Turn smart phones into a botnet

Last year researchers found the NFL mobile app exposed users personal information via a MITM attack before last year’s Super Bowl.^{iv} Concurrently, there can also be in-game issues. During the January 24 AFC championship game between the Broncos and Patriots, the Patriots experienced issues with their tablets issued by the NFL to coaches to review plays.

How to Prepare

Technology can provide a more immersive and rewarding experience for fans, but also create problems and security risks for those managing the event. Here are suggestions for both attendees and stadium management/wireless network providers supporting Super Bowl 50.

Attendees/Users: How to prepare for Super Bowl 50

- Ensure your phone is updated with the latest operating system
- Disable Bluetooth when not in use
- Disable Wi-Fi when not in use
- Use the stadium’s Wi-Fi when device is in use
- Use VPN
- Have RFID shields to protect RFID cards
- Be careful when using ATMs – Understand how to spot and avoid card skimmers gathering card data at stadium ATMs.
- Exercise caution when presented with pop ups while browsing

Stadium Operators: How to prepare for Super Bowl 50

We recommend that stadium operators review their network between events and inspect networks as necessary in order to defend the threats presented in a smart stadium.

- Ensure hardware is up to date
- Regularly patch devices in the stadium
- Conduct audits of the network between games
- Access Control List (ACL) – Filtering network traffic
- Use load balancing for traffic distribution
- Have network and application protection to detect, mitigate and report

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report today’s most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware’s attack mitigation solutions can better protect your network [contact us](#) today.

ⁱ <http://www.mobilesportsreport.com/2015/02/super-bowl-xlix-sets-new-stadium-wi-fi-use-record-with-6-2-terabytes-of-data-consumed/>

ⁱⁱ http://about.att.com/story/enhances_bay_area_mobile_coverage_big_game.html

ⁱⁱⁱ <http://www.forbes.com/sites/kurtmarko/2015/01/08/levis-mobile-experience/#7d5641986e6d>

^{iv} <http://www.securityweek.com/super-bowl-fans-warned-about-vulnerable-nfl-mobile-app>