WHITE PAPER

Security Challenges of University Environments

SecureWorks® Counter Threat Unit™ Threat Intelligence

SecureWorks

Executive Summary

University networks are attractive targets due to their large bandwidth and the types of information they store and transmit. This information includes personal and financial data about students, staff, and alumni; details about potentially valuable research projects and intellectual property; and healthcare data from connected medical centers. The range of possible access vectors also appeals to attackers. Students' personal computers may have outdated or lax security, and regular data transmission via the network and removable media create many propagation vectors for malware. Unmanaged computers must connect to the core university network to access educational services.

Individuals who have been charged with securing an enterprise know that the challenges can be significant. An attacker needs to find only one weakness to exploit, while the defender is tasked with eliminating all weaknesses.

The complexity of a university environment magnifies this challenge and introduces a number of impediments to optimizing defense.

Network Segments

A university environment could be described as a collection of related enterprise networks with potentially loose couplings but coordinated purpose and usage. Compared to other enterprise networks, it is typically more distributed due to organizational boundaries yet fairly flat due to the need for interconnectedness and academic freedom (see Figure 1). This combination amplifies weaknesses. Another aspect that is somewhat unique to the university environment is the broad variety of roles: students, administrators, faculty, visiting researchers, event attendees, and general public. Each role has specific needs for networking resources but should have different levels of authorization. As a result, permissions should be role-based to provide the least-permissive access to each individual while still providing necessary services.

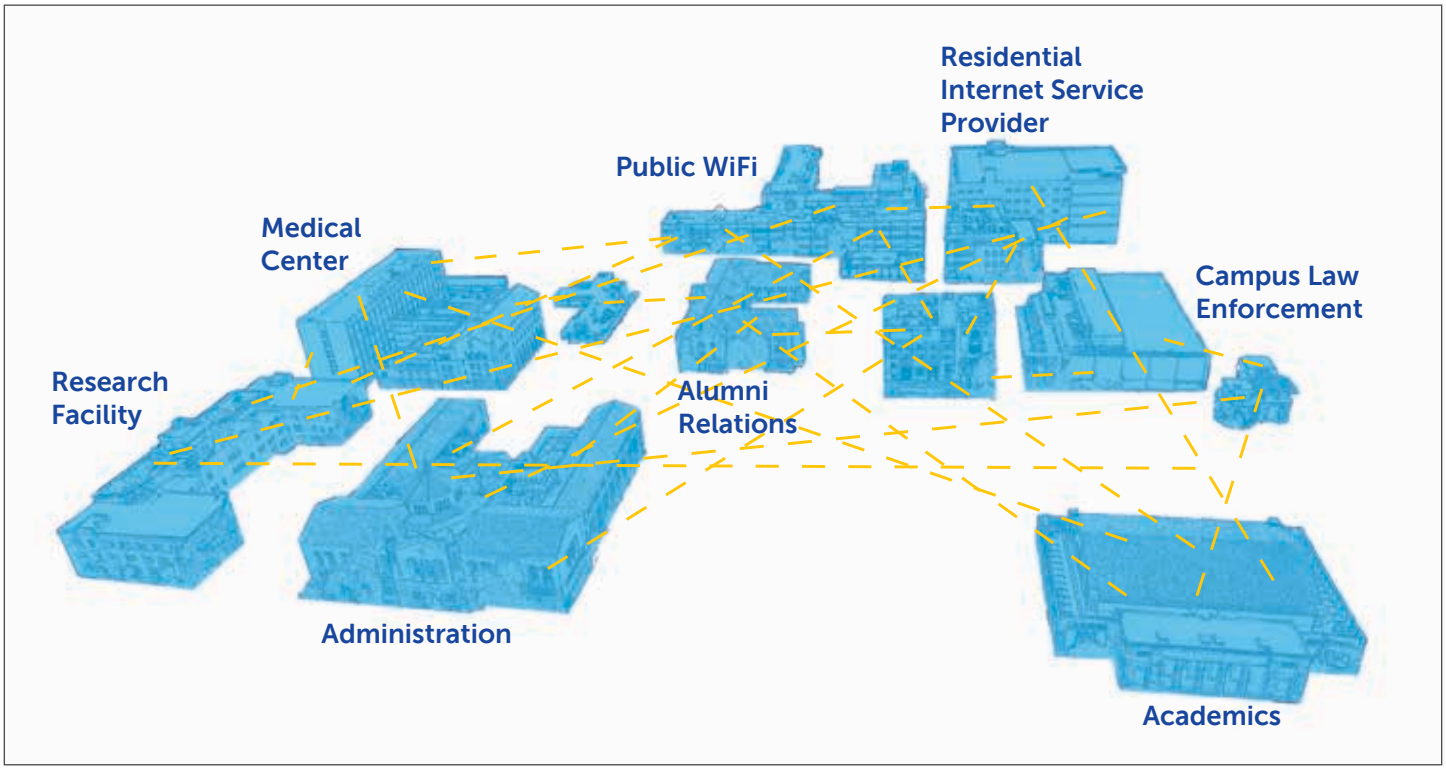
What You Will Learn

- Complexities of interconnectivity
- The assets that need to be protected by department
- How to protect those assets
- Best practices that can increase the overall security of your university

Who Should Read This White Paper

- CISO/CSOs
- Directors of Security
- Security Architects

Figure 1. The complexities of interconnectivity. (Source: SecureWorks)



Many universities have department-based IT and computer security staff that might not coordinate best practices or implementation, and some administrators may have to relax controls to ensure services remain available. Further, academic freedom, tenured faculty conducting research, the introduction of emerging services, and budget considerations can add additional complications for security and IT. Viewing the environment as a collection of smaller networks with distinct purposes and services can make the segments easier to secure and can facilitate decisions about how to expose specific services to other segments of the network while managing risk and complying with any applicable external data-handling regulations (e.g., HIPAA).

Administration

The network segment used by the university administration may be the easiest to secure. The hardware and software is likely owned by the school and used by employees with employment agreements. The application of standard hardware images and approved software provide a strong security baseline that can be augmented. The best managed environments implement departmental isolation by role, centralized systems management, endpoint protection, and network monitoring.

Academics and IT Operations

Academics and IT operations (e.g., email, intranet, teacher pages) are integral to a university environment. These services are generally well understood and have established best practices for security and configuration. Although they require interconnectedness across network segments, it should be possible to implement a constrained design that limits access. For example, because the users of these services have a direct contractual relationship with the university, either as employees or students, two-factor authentication should be fairly straightforward. Many university environments provide constituents with either a student ID or other form of cardkey that could be leveraged as a security token. In cases where that is not practical, mobile devices could be used as a second form of access control (via SMS or an authentication app).

Research

Advanced research projects can be valuable to foreign governments or unscrupulous corporations willing to invest significant resources to obtain specific intelligence. Research environments may have long-running experiments, data collection, or other aspects that make scheduling ongoing security maintenance difficult. Further, those systems may have been purchased with grant money, removing the control and security management from the university's centralized IT administration. The lack of management but requirements to access the public Internet and core university services reinforce the need to expose services such as email and internal websites to network segments in a constrained manner with additional safeguards in place. Adding layers of defense, control, and monitoring at access points within the university's control minimizes the risks that an unmanaged system poses to the larger network while providing the required access to services. Departments should determine what intellectual property is at greatest risk of compromise and implement appropriate security measures to protect information, such as keeping the data off the network.

Financial Management

Universities' financial systems can be as attractive to criminals as banks. Endowments, grants, faculty payroll, and property management provide lucrative opportunities if they are not adequately protected. The relationship between financial management and other segments of the university may necessitate connectivity to environments with different levels of security, so it is important to implement a model of least privilege and regularly monitor connection points. Processes defining how data interchange and service delivery occurs should be implemented to easily identify and address anomalies.

Campus Law Enforcement

Many universities employ physical security teams or law enforcement to police the grounds and keep people safe. These individuals create reports and files about incidents that need to be accessible to a small number of people in campus security and university administration while remaining private from others. In many cases, these goals are best achieved by completely isolating law enforcement systems on a different network that is separated from the rest of campus systems.

Residential ISP

Dormitories, apartments, and other campus housing may be the most difficult segments of a university network to protect. The influx of new unmanaged systems each term increases risk due to the inability to force configuration or device type, the likelihood of risky online behaviors by the users, and students' expectation of unrestrained access to the Internet and school resources. Segmentation and isolation provide the best recourses for defense.

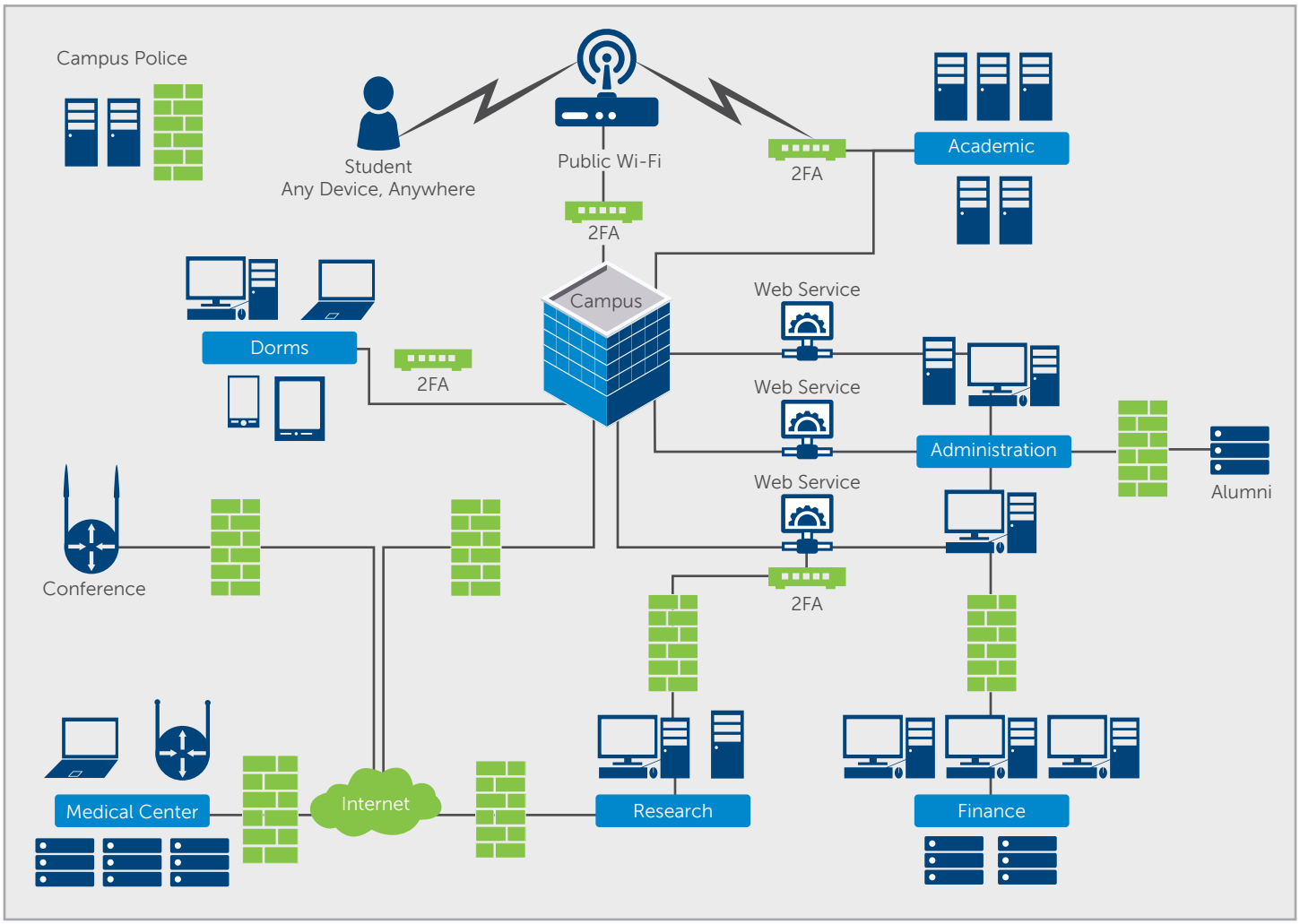
Alumni Relations

Universities often maintain information about previous students, including graduation year, degree, current address, and possibly job history. Attackers could use this information to craft convincing spearphishing campaigns. There is also a large market for financial information such as past donations in the underground economy. It may be appropriate and straightforward to isolate the alumni services segment as there is minimal need for access to services in other segments of the university network.

Conferences

Many universities host conferences for both internal and external constituents, and these ad hoc events may have their own networking requirements. IT and security staff should design a secure reference model for each conceivable type of event: internal with access to university resources, external with access limited to the Internet, and other possible combinations. The best designs verify access, such as providing individual credentials to each participant during registration or at check-in and limiting access to confirmed participants. Controls that limit access for these temporary networks are essential. Although creating and monitoring these networks may burden IT resources, the investments guard against unexpected time, effort, and consequences (e.g., data loss, network downtime) associated with managing and recovering from incidents.

Figure 2. Simplification of design can expose logical relationships between segments. (Source: SecureWorks)



Public Wi-Fi

Students and faculty may expect to have access to network resources from any point on campus via various device types. Due to the unknown security posture of those devices, it is essential to implement narrow connection points to services as well as enhanced monitoring. A separate network for public access to campus Wi-Fi creates the opportunity for more secure network designs through isolation.

Medical Center

Many large universities have a medical center that serves the internal community or the surrounding public community. A medical center creates additional challenges due to compliance requirements governing the protection of health information. Embedded systems in medical devices may have certifications that do not allow updates, complicating security implementation. There are also often connections to external parties such as insurers to process claims, Wi-Fi connections for patients and family, and shared systems associated with patient care that can be left unlocked and loosely monitored by medical staff.

These environments likely do not require access to core university services but sometimes need access to research segments. Medical center segments must be isolated from other segments and may require a different approach to workstation management, such as virtualized images that IT regularly updates and workstations that are refreshed at shift change. Proximity cards and biometric logins for staff could avoid patient care delays caused by typing a complex password. Patient care systems should be segregated from any Internet access offered to patients and their families, and systems with protected health information should be further isolated with access granted only to those with a direct business need.

Recommendations

Although all standard best practices for securing an enterprise apply, the following represent ways to increase the overall security of the university network environment while providing services on demand:

- Segment networks and limit access and privileges using role-based access controls when possible. Pay particular attention to separating managed and unmanaged systems.
- Coordinate design, implementation, monitoring and response across partner networks.
- Filter traffic between networks.
- Keep current with security updates on managed systems. Educate administrators of self-managed systems about how to access and apply updates. Consider offering self-help tools to check compliance status.
- Understand and deploy appropriate security solutions, ensuring consistency with threat modeling and risk reduction plans.
- Understand "normal" network behavior and monitor for anomalies. Invest in a robust security monitoring and incident response capability that includes endpoint threat detection.
- Where business demands prohibit preventive control, consider substituting with a detective control.
- Identify potential adversaries and apply knowledge of their motivations and their tactics, techniques and procedures (TTPs) to network and security decisions.
- Educate users about risks and responsibilities associated with network usage. Train staff and students how to recognize and respond to threats such as phishing attempts.
- Leverage network access control technologies to remove systems identified as threats from the network. Provide a self-help mechanism for students and other owners of unmanaged systems to understand and remediate identified issues.
- Consider packet-shaping technology to control bandwidth consumption by sharing and streaming protocols, or by distributed denial of service (DDoS) attacks that could impact key academic services.
- Review strategies to rapidly recover managed systems after destructive threats such as ransomware encryption.

Understanding who needs access to what and under which circumstances can provide a baseline for design. Additional knowledge about devices and services enables IT personnel to design and deploy systems that provide robust solutions to constituents while minimizing risk from unauthorized access.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com