

3

IT Security Technologies Implemented by Higher Education Institutions

It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something.

—Franklin D. Roosevelt

Key Findings

- ◆ Network perimeter firewalls, centralized data backup systems, virtual private networks (VPNs), enterprise directories, and network interior firewalls are the technologies most in use.
- ◆ Use of active filtering, VPNs for remote access, and enterprise directories all increased markedly since 2003.
- ◆ Doctoral institutions are less likely to employ network perimeter firewalls and are more likely to have installed intrusion detection and a VPN. The implementation of firewalls is significantly higher in 2005 than in 2003.
- ◆ There is significantly less difference among Carnegie class institutions in the use of IT security technologies in 2005 compared with 2003.
- ◆ The most significant change in wireless security between 2003 and 2005 is the increased implementation of firewalls, followed by IP VPNs.
- ◆ Conventional passwords/PINs continue to predominate. More than one-quarter of responding institutions used Kerberos.
- ◆ The most often used IT security strategies were limiting protocols allowed through the network firewall or router, restricting or limiting access to servers and applications, and timing-out access to applications after an idle period.
- ◆ Fewer than half of respondents reported having a disaster recovery plan.

This chapter explores the status of information security technologies in use by the 492 institutions in our survey. What tools have they chosen to install to prevent harm to their information assets? Do we find differences among the institutions? For example, do different Carnegie class institutions pursue

different IT security strategies? What has changed and at what rate between 2003 and 2005? And how does higher education compare with industry? Is it true that higher education lags the private and corporate sector in installing security technologies? And if so, is it really an issue?

©2006 EDUCAUSE. Reproduction by permission only.

Technologies in Use

The data we have collected portray a fairly comprehensive view of security approaches that our subset of higher education institutions currently have in place, are implementing, or are piloting for the purpose of preventing cyber attacks. For institutions in the planning stage, we queried when they planned to undertake various security approaches. We also

determined whether an approach was even under consideration (see Table 3-1). Note that our survey's data closely mirror those reported in the 2005 EDUCAUSE core data survey, which reinforces the representativeness of the data used in this study.

Table 3-1 presents the data on IT security technologies in rank order of use. Network perimeter firewalls, centralized data backup

Table 3-1. Status of Security Approaches Used by Participating Institutions (N = 492)

	Already Implemented	Implementation in Progress	Will Implement within 12 Months	Not Planning to Implement within 12 Months	Don't Know
Network firewalls (perimeter)	83.4%	5.3%	2.0%	8.3%	0.8%
Centralized data backup system	76.4%	10.7%	4.5%	7.4%	0.8%
Virtual private network (VPN) for remote access	74.6%	10.8%	7.0%	6.1%	1.4%
Enterprise directory	68.3%	14.5%	5.7%	6.5%	4.5%
Network firewalls (interior)	66.1%	13.7%	5.3%	13.5%	1.4%
Active filtering	57.8%	6.6%	7.2%	16.9%	11.5%
Intrusion detection	55.7%	17.0%	15.2%	9.8%	2.3%
Encryption—transmission	49.4%	18.9%	8.4%	16.8%	6.6%
Digital certificates	47.7%	11.7%	9.8%	21.5%	9.2%
Application layer firewalls (such as Web server firewall)	46.0%	11.3%	5.8%	28.7%	8.2%
Security event management (centralization of logging, collection, and monitoring of various IT events)	41.2%	18.9%	18.0%	17.4%	4.5%
Intrusion prevention	39.8%	15.8%	19.7%	19.9%	4.9%
Security standards for application or system development	32.2%	19.1%	16.2%	23.6%	8.8%
Encryption—data storage	13.5%	13.1%	14.5%	47.3%	11.5%
Electronic signature	7.4%	10.3%	13.4%	56.9%	12.0%
Shibboleth	2.7%	5.6%	9.1%	59.1%	22.9%

systems, VPNs, an enterprise directory, and network interior firewalls are most in use or under way. Electronic signatures are either not under consideration or are, at best, 12 months out. And the lowest score is given to Shibboleth, with only 2.7 percent of the respondents having implemented it. Note that these percentages (excluding Shibboleth) are quite similar to the responses of *CIO Magazine's* survey of 8,200 IT professionals in 62 countries (see <<http://www2.cio.com/research/surveyreport.cfm?id=95>>).

We counted the number of security approaches implemented at each institution and found the average to be 7.5 of the 16 IT security approaches or technologies included in this study. One institution reported having implemented all 16; 5.0 percent reported having implemented 13 or more approaches; 10.0 percent reported having implemented three or fewer. The average was the same for each Carnegie class, although the mix of approaches differs, as we show later in Table 3-3.

We also looked to see whether respondents followed through on plans to implement a particular approach. For the 204 institutions that responded to the 2003 and 2005 surveys, those that indicated they were planning to implement an approach in the next year or were in the process of implementation did, for the most part, what they indicated they planned to do. And those respondents not planning to implement a particular approach, even more so, did not. Institutions are not “doing by planning!”

Note, too, that of the respondents having implemented interior firewalls, 86.6 percent have also installed network perimeter firewalls. Of the institutions that have installed network perimeter firewalls, 68.4 percent have also installed interior firewalls. Two institutions in our study had no firewalls and did not plan to implement them. Instead, they apparently rely on application-layer firewalls. Ten institutions without network perimeter

and interior network firewalls were in the process of implementing one or the other.

New Adopters and Rates of Change

Since 2003, the number of attacks on university networks has accelerated in severity and sophistication, and in many instances software, hardware, services, and data have been damaged. We expected to find aggressive changes to security hardware and software acquisition and implementation, and we did (see Table 3-2). We compared security approaches adopted in 2003 with those for 2005 and listed them in the order of most used in 2005—from network perimeter firewalls (highest) to Shibboleth (lowest).

The rank order shifted slightly from 2003 to 2005, with VPNs, active filtering, and intrusion detection moving up in rank order of use. These approaches had the highest percentage of new adopters—in excess of 16 percent.

Noteworthy, too, is the rather dramatic percentage change when viewed by approach. Active filtering increased by 99.7 percent, VPN for remote access by 65.4 percent, and enterprise directories by 55.3 percent. Even highly used network perimeter firewalls showed a significant rate of change of 13.1 percent, and network interior firewalls increased by 27.5 percent. The growth rate of Shibboleth is considerable but inconclusive because of the overall low number of users in the base year 2003.

Mark Bruhn, Indiana University associate vice president for telecommunications and associate director, IU Center for Applied Cybersecurity Research (and until recently chief IT security and policy officer), notes that these dramatic changes describe Indiana University to a tee. IU expanded VPN service, and all wireless use now requires VPN. “And we absolutely deploy active filtering. We have a lot of automated scripts analyzing netflow data nightly, aggressively looking for vulnerabilities

Table 3-2. Change in Security Approaches Used by the 204 Institutions in the 2003 and 2005 Studies (N = 204)

IT Security Approach	Percentage Used in 2005	Percentage Used in 2003	Percentage New Adopters	Rate of Change 2003–2005
Network firewalls (perimeter)	77.0%	68.1%	8.9%	13.1%
Centralized data backup system	76.6%	68.1%	8.5%	12.5%
Virtual private network (VPN) for remote access	75.4%	45.6%	29.8%	65.4%
Enterprise directory	71.9%	46.3%	25.6%	55.3%
Network firewalls (interior)	65.0%	51.0%	14.0%	27.5%
Intrusion detection	62.3%	46.1%	16.2%	35.1%
Active filtering	59.3%	29.7%	29.6%	99.7%
Intrusion prevention	44.3%	33.5%	10.8%	32.2%
Security standards for application or system development	32.4%	27.5%	4.9%	17.8%
Electronic signature	6.4%	5.9%	0.5%	8.5%
Shibboleth	4.9%	1.5%	3.4%	226.7%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

and anomalies. Results are reported every morning in terms of potential problems, and there are staff assigned to interact with users of those machines. And, depending on the level of risk to other systems, some of the trouble machines identified are automatically isolated.” Router filters for problematic protocols have been in place for a long time (passive filtering). The enterprise directory is being used much more than ever. They have created “security enclaves for critical systems. Every device on the IU network—IUB and IUPUI campuses to start—will have to be registered and known on the database. Technical support people for these systems have to be identified as well. Thus they can identify problems and who to call in response to a problem. IU also hosts the Research and Educational Networking Information Sharing and Analysis Center (REN-ISAC),

which has as its basic goal assisting other campuses to defend their local networks.”

We then clustered the approaches by their penetration in higher education and their growth rate (see Figure 3-1). A high penetration rate is defined arbitrarily as having reached more than 50 percent of the market, and a high growth rate is defined as more than 50 percent over two years. By virtue of their high growth rate, VPN for remote access, enterprise directories, and active filtering all have a high penetration rate. Network perimeter firewalls were heavily in use in 2003, so the growth rate is lower. However, their use at doctoral institutions increased significantly (see Table 3-4). Electronic signatures have both low market penetration and a low growth rate. Shibboleth has a high growth rate but currently very low market penetration.

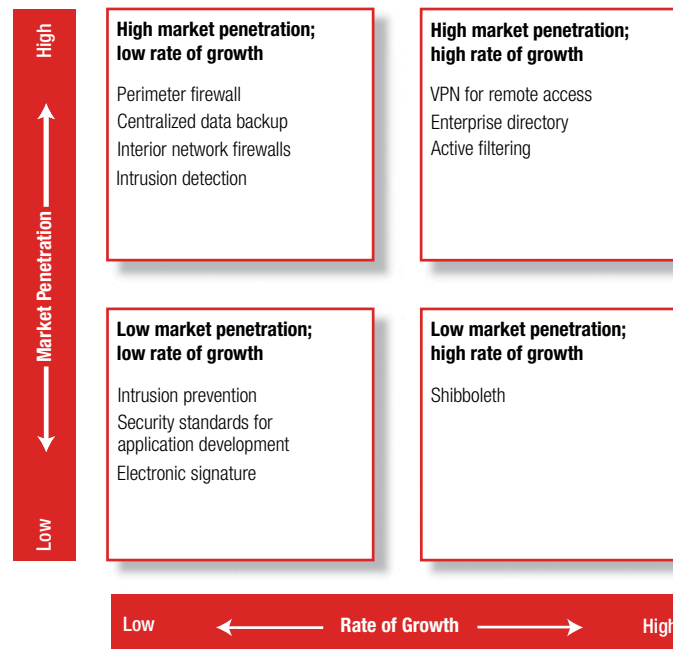


Figure 3-1.
Security Approach
Market Penetration
and Growth Rate,
2003 to 2005
(N = 204)

We looked for differences by Carnegie class and Canadian respondents (see Table 3-3), and a few findings are noteworthy. Doctoral institutions are still less likely to employ network perimeter firewalls and are more likely to have installed intrusion detection and VPN. The implementation of firewalls is significantly higher than in 2003, and that is true for all respondents. BA institutions report a higher deployment of enterprise directories. Canadian institutions report higher numbers for centralized data backup, and the 87.9 percent they reported for 2005 compares markedly with 61.9 percent in 2003.

What is remarkable is the overall similarity of use across Carnegie class, which was not the case in 2003. And we can explain that outcome by the remarkable adoption rate of IT security approaches by MA, BA, and AA institutions in the last two years (see Table 3-4). These data validate our prediction in the 2003 study (Kvavik & Voloudakis, 2003) that many institutions would need to rethink their security management, as the nature of security threats changed from individual hack-

ers targeting specific institutions to automated attacks that indiscriminately penetrate any unprotected system attached to the Internet. Such attacks have leveled the playing field, mandating that any organization attached to the Internet have a minimum level of protection in place to survive.

We rank ordered the IT security approaches in use as a way to demonstrate where approaches differed (see Table 3-5). Doctoral institutions differed in the use of VPNs, intrusion detection, and perimeter firewalls. The AA, BA, MA, and Canadian institutions were a third more likely than doctoral institutions to have perimeter firewalls. Institutions with smaller FTE enrollments were more likely to use firewalls (perimeter and interior).

Perimeter firewall usage has increased by 21.6 percent at responding doctoral institutions, and this represents a major change from 2003. At that time, the argument was for open networks, closed servers, and protected sessions. Some large institutions have still chosen to stay with a host-based rather than a perimeter-based security model. The

host-based model achieves tighter security by tailoring security to the specific application or needs of each small group or individual.

VPNs provide the ability to create an encrypted tunnel across a network connection, providing a point-to-point secure connection across an otherwise public network such as the Internet or the internal campus network. VPN was in place at 74.6 percent of all responding institutions (see Table 3-1), with doctoral institutions highest at 83.3 percent (see Table 3-3). Note that our data do not include this technology's penetration rate; some institutions may deploy VPNs broadly, while others may make them available only to specific campus segments.

VPN technologies can be used for several purposes. For remote (off-campus) users, they provide a secure connection to resources on the institution's network via an encrypted path through the perimeter firewall. However, since VPN solutions require the deployment of client software and payment of per-user license fees, institutions may choose to require VPNs only for direct access to sensitive systems, such as enterprise resource planning (ERP) systems, instead employing SSL-based encryption for access to common resources such as e-mail or self-service applications. VPN technologies can also be employed within the campus network to provide additional protection for sensitive data. For example, users with access

Table 3-3. IT Security Approach Already Implemented, by Carnegie Class (N = 446)

IT Security Approach	DR	MA	BA	AA	Canada
Network firewalls (perimeter)	59.7%	90.0%	93.0%	94.7%	84.8%
Network firewalls (interior)	64.2%	70.0%	70.6%	64.0%	57.6%
Application-layer firewalls (such as Web-server firewall)	47.0%	47.7%	47.1%	48.6%	45.5%
Enterprise directory	67.5%	66.9%	79.1%	64.0%	75.8%
Electronic signature	7.6%	6.2%	6.1%	8.1%	6.1%
Shibboleth	7.6%	0.0%	1.2%	1.4%	3.0%
Encryption—transmission	47.9%	46.5%	51.2%	50.7%	54.5%
Encryption—data storage	13.3%	10.8%	9.5%	20.0%	18.2%
Centralized data backup system	73.1%	77.7%	76.8%	76.0%	87.9%
Virtual private network (VPN) for remote access	83.3%	72.1%	65.1%	66.7%	74.6%
Security standards for application or system development	33.6%	29.2%	32.6%	32.4%	39.4%
Intrusion detection	70.0%	54.6%	47.7%	49.3%	42.4%
Intrusion prevention	47.5%	35.4%	39.5%	36.5%	34.4%
Active filtering	58.3%	56.9%	65.5%	54.1%	54.5%
Security event management (centralization of logging, collection, and monitoring of various IT events)	45.8%	41.5%	36.0%	33.8%	51.5%
Digital certificates	36.7%	55.8%	47.7%	55.4%	45.5%

Table 3-4. Increase in Adoption by Carnegie Class for IT Security Approaches, 2003 to 2005 (N = 204)

IT Security Approach	DR	MA	BA	AA	Canada
Network firewalls (perimeter)	21.6%	11.4%	6.7%	12.5%	11.1%
Network firewalls (interior)	33.3%	34.8%	12.1%	85.9%	0.0%
Enterprise directory	50.1%	114.9%	45.1%	66.5%	66.8%
Centralized data backup system	7.4%	16.6%	25.9%	6.6%	42.9%
Virtual private network (VPN) for remote access	47.7%	98.1%	140.3%	100.0%	0.0%
Security standards for application or system development	46.9%	43.7%	21.9%	16.0%	74.7%
Intrusion detection	21.8%	91.6%	23.7%	180.2%	33.2%
Intrusion prevention	34.8%	83.3%	27.4%	124.6%	25.0%
Active filtering	136.8%	65.6%	86.6%	146.0%	49.7%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 3-5. Rank Order of IT Security Approach, by Carnegie Class (N = 446)

IT Security Approach	DR	MA	BA	AA	Canada
Virtual private network (VPN) for remote access	1	3	6	3	4
Centralized data backup system	2	2	3	2	1
Intrusion detection	3	8	9	9	11
Enterprise directory	4	5	2	4	3
Network firewalls (interior)	5	4	4	5	5
Network firewalls (perimeter)	6	1	1	1	2
Active filtering	7	6	5	7	6
Encryption—transmission	8	10	7	8	7
Intrusion prevention	9	12	11	11	13
Application-layer firewalls (such as Web-server firewall)	10	9	10	10	10
Security event management (centralization of logging, collection, and monitoring of various IT events)	11	11	12	12	8
Digital certificates	12	7	8	6	9
Security standards for application or system development	13	13	13	13	12
Encryption—data storage	14	14	14	14	14
Electronic signature	15	15	15	15	15
Shibboleth	16	16	16	16	16

to sensitive data could be required to use a VPN to access internal systems or to make connections across a wireless network.

Shibboleth, a project of Internet2/MACE (Middleware Architecture Committee for Education), is developing architectures, policy structures, practical technologies, and an open source implementation to support interinstitutional sharing of Web resources, subject to access controls. Using Shibboleth, the origin campus (home to the browser user) provides attribute assertions about that user to the target site. A trust fabric exists between campuses, allowing each site to identify the other participant and assign a trust level. Origin sites are responsible for authenticating their users but can use any reliable means to do so. Access control decisions are made using those assertions. The origin site and the browser user control what information is released to the target. For more on Shibboleth, see <<http://shibboleth.internet2.edu/>>.

In the ongoing war to protect digital assets, new tools are continually on the horizon. For example, George Washington University will soon implement a tool called Recognix that monitors the packets on its network, sees where confidential information is going, and stops it if it is not authorized to go outside the network. Even if an infection or compromise exists, information can be stopped from leaving the network, making the compromise more benign.

We compared our ECAR survey findings with those of the 2005 CSI/FBI Computer Crime and Security Survey, sponsored by the Computer Security Institute (see <<http://www.gocsi.com/press/20050714.jhtml>>). The comparison is difficult, as we have used a far more refined instrument to identify IT security technologies in use. Moreover, higher education institutions face a different risk profile and therefore may require a somewhat different set of solutions. The CSI survey shows higher network firewall use, but this is likely due to the doctoral institutions in our

survey being less inclined to use firewalls and to provide security closer to the application. In contrast, higher education is more likely to deploy intrusion prevention systems. Use of antivirus software is identical, with nearly universal penetration.

Wireless IT Security

The proliferation of wireless technologies and infrastructure has created additional IT security and operational challenges for the central IT office. According to Chris Misra, network analyst at the University of Massachusetts at Amherst, "Given the proliferation of wireless access points, the traditional security boundary is lost. In the wired environment one can often tie a problem back to a specific physical location, but this is not possible in the wireless realm. Our ability to detect rogue access points is problematic. User education is the most workable approach we currently have. Hopefully, a broader deployment of newer-generation wireless infrastructure with the capability of detecting and possibly disabling the rogue access point will help us to solve this challenge."

Table 3-6 shows what our respondents have implemented, are implementing, plan to implement, and are not implementing. The primary tool is firewalls (71.4 percent), followed by remote authentication dial-in user service (RADIUS) at 54.4 percent. Least used is Advanced Encryption Standard (AES) at 14.2 percent, although the rate of change is significant (see Table 3-7), especially at doctoral institutions and in Canada (see Table 3-9).

As Table 3-7 shows, the most significant change in wireless security between 2003 and 2005 is the implementation of firewalls (32.7 percent new adopters), followed by IP VPN (21.6 percent). Noteworthy, too, is the overall positive increase in implementation of all strategies. The positive rate of change is dramatic, ranging from 10.7 percent to 193.5 percent.

The rate of change is even more dramatic when we compare 2005 results with ECAR's

Table 3-6. Wireless Security Protection (N = 492)

Wireless Security Protection	Already Implemented	Implementation in Progress	Will Implement within 12 Months	Not Planning to Implement within 12 Months	Don't Know
Firewall	71.4%	6.6%	4.3%	13.7%	3.9%
Remote authentication dial-in user service (RADIUS)	54.4%	2.9%	6.5%	29.0%	7.3%
Internet protocol virtual private network (IP VPN)	47.8%	10.5%	7.4%	25.3%	9.1%
Registration of MAC	47.1%	8.3%	7.5%	30.0%	7.1%
128-bit Wired Equivalent Privacy (WEP)	34.5%	6.7%	5.9%	42.7%	10.3%
Wireless vendor supplied proprietary solution	25.7%	5.7%	5.7%	50.1%	12.7%
Kerberos	21.2%	3.2%	5.1%	56.9%	13.6%
Extensible Authentication Protocol (EAP)	19.7%	8.5%	13.4%	41.6%	16.8%
40-bit Wired Equivalent Privacy (WEP)	19.6%	1.9%	1.9%	63.4%	13.2%
Advanced Encryption Standard (AES)	14.2%	5.5%	12.1%	47.9%	20.3%

2002 study of wireless networking in higher education (Arabasz & Pirani, 2002) based on data collected from 299 institutions in 2001 (see Table 3-8). We caution the reader that the Carnegie mix of institutions is different and so the data must be read cautiously. But we think the trend is correct. Excluding 40-bit and 128-bit WEP, the rates of change range from 208.8 percent to 773.3 percent. Firewalls, RADIUS, and IP VPN have high market penetration and an enormous growth rate. The percentages for Kerberos and EAP should also be read with caution because of the low percentage of use in 2001.

Based on Table 3-7, we then clustered the approaches by their penetration into the higher education market and their growth rates (see Figure 3-2). By virtue of their high

growth rate, firewalls and IP VPN have a high penetration rate. WEP has low market penetration and a low growth rate, while AES and EAP have high growth rates but currently very low market penetration.

We also looked for difference in use by Carnegie class. With some exceptions, a higher percentage of doctoral institutions are using wireless security technologies, as shown in Table 3-9. This may in part be explained by these institutions' greater wireless deployment. Note the significantly higher percentage of use of RADIUS, IP VPN, Kerberos, and AES at the doctoral institutions. Note, too, that while the percentage of use differs, the pattern of use is quite similar, much more so than what we demonstrated in Table 3-5 (see Table 3-10).

Table 3-7. Wireless Security Protection Adoption and Rate of Change, 2003 to 2005 (N = 204)

Wireless Security Protection	Percentage Used in 2005	Percentage Used in 2003	Percentage New Adopters	Rate of Change 2003–2005
Firewall	74.1%	41.4%	32.7%	79.0%
Internet protocol virtual private network (IP VPN)	51.5%	29.9%	21.6%	72.2%
Remote authentication dial-in user service (RADIUS)	50.8%	45.9%	4.9%	10.7%
128-bit Wired Equivalent Privacy (WEP)	39.5%	29.6%	9.9%	33.4%
Wireless vendor supplied proprietary solution	28.6%	18.2%	10.4%	57.1%
Kerberos	26.2%	13.2%	13.0%	98.5%
Extensible Authentication Protocol (EAP)	22.6%	7.7%	14.9%	193.5%
40-bit Wired Equivalent Privacy (WEP)	21.1%	17.5%	3.6%	20.6%
Advanced Encryption Standard (AES)	18.9%	4.4%	14.5%	125.4%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 3-8. Wireless Security Protection Adoption and Rate of Change, 2001 to 2005 (N = 492 for 2005; N = 299 for 2001)

Wireless Security Protection	Percentage Used in 2005	Percentage Used in 2001	Rate of Change
Firewall	74.1%	24.0%	208.8%
Remote authentication dial-in user service (RADIUS)	65.5%	18.0%	263.9%
Internet protocol virtual private network (IP VPN)	51.5%	14.0%	267.9%
128-bit Wired Equivalent Privacy (WEP)	39.5%	33.0%	19.5%
Wireless vendor supplied proprietary solution	28.6%	9.0%	217.8%
Kerberos	26.2%	3.0%	773.3%
Extensible Authentication Protocol (EAP)	22.6%	5.0%	352.0%
40-bit Wired Equivalent Privacy (WEP)	21.1%	17.0%	24.1%

Note: Comparisons of changes between 2001 and 2005 are based on data from the 492 institutions that participated in the 2005 study and 299 institutions that participated in the 2001 study.

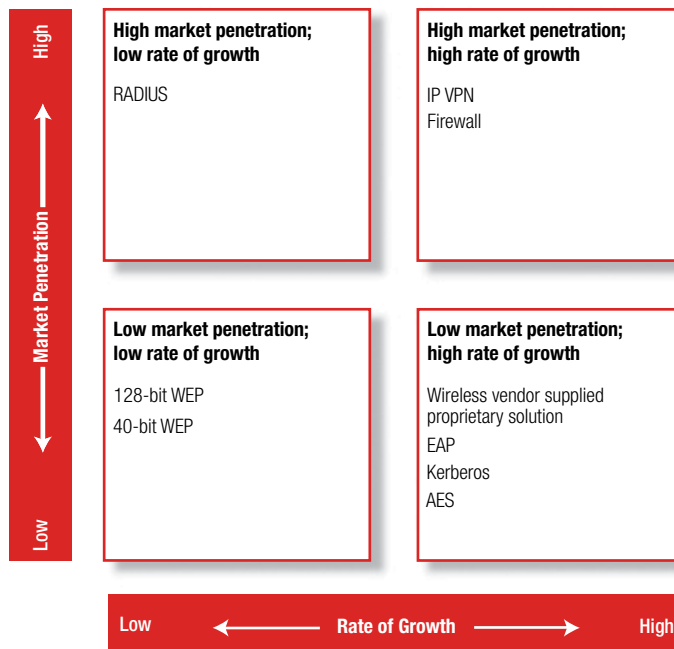


Figure 3-2.
Wireless Security Market Penetration and Growth Rate, 2003 to 2005 (N = 204)

Table 3-9. Wireless Security, by Carnegie Class and Canada (N = 446)

Wireless Security Protection	DR	MA	BA	AA	Canada
Remote authentication dial-in user service (RADIUS)	71.4%	53.1%	54.9%	33.8%	53.1%
Firewall	70.6%	70.3%	71.4%	74.3%	72.7%
Internet protocol virtual private network (IP VPN)	59.3%	45.2%	37.8%	37.3%	47.8%
128-bit Wired Equivalent Privacy (WEP)	34.7%	27.0%	32.1%	39.2%	34.5%
Kerberos	32.5%	18.3%	14.4%	16.7%	21.2%
Wireless vendor supplied proprietary solution	25.6%	24.2%	25.6%	23.6%	31.3%
40-bit Wired Equivalent Privacy (WEP)	21.4%	16.0%	18.5%	16.7%	25.8%
Advanced Encryption Standard (AES)	20.3%	11.3%	8.5%	11.0%	21.9%
Extensible Authentication Protocol (EAP)	18.3%	17.2%	19.8%	13.7%	32.3%
Registration of MAC	54.6%	50.0%	60.0%	37.8%	37.5%

Table 3-10. Rank Order of Wireless Security, by Carnegie Class and Canada (N = 447)

Wireless Security Protection	DR	MA	BA	AA	Canada
Firewall	2	1	1	1	1
Remote authentication dial-in user service (RADIUS)	1	2	3	5	2
Internet protocol virtual private network (IP VPN)	3	4	4	4	3
Registration of MAC	4	3	2	3	4
128-bit Wired Equivalent Privacy (WEP)	5	5	5	2	5
Extensible Authentication Protocol (EAP)	10	8	7	9	6
Wireless vendor supplied proprietary solution	7	6	6	6	7
40-bit Wired Equivalent Privacy (WEP)	8	9	8	7	8
Advanced Encryption Standard (AES)	9	10	10	10	9
Kerberos	6	7	9	8	10

The rates of change are dramatic across the board (see Table 3-11), in particular for EAP, firewalls, Kerberos, and AES.

Again, we see even more dramatic rates of change when we compare these data with those from ECAR's 2001 study of wireless networking in higher education (Arabasz & Pirani, 2002) (see Table 3-12). The greatest rate of change overall has been among BA respondents. The data provide further evidence that IT security differentiation among Carnegie class institutions in 2005 is significantly less than in 2001.

Doctoral and Canadian institutions have deployed more wireless technologies than their counterparts, and AA institutions have deployed the fewest (see Table 3-13). On average, the institutions in our survey have implemented between three and four of the 10 technologies identified. Again, we believe this is attributable to earlier and broader deployment of wireless at these institutions.

We asked Chris Misra at the University of Massachusetts at Amherst about expected changes in this area in the next several years. He expects to be looking at IEEE 802.1x

technology for authentication in the future as well as active filtering to complement a less intrusive analysis of net flow data. A particular challenge is accommodating the needs of students and faculty in a five-college consortium, to which UMass Amherst belongs. Eduroam.org, currently serving Europe, Australia, and Taiwan, offers a model for authentication while visiting another campus. Eduroam.org is considering a federated approach, noting that The University of Texas System has been trying to deploy Shibboleth with RADIUS. In addition to the University of Texas, an Internet2 working group, Federated Wireless NetAuth (FWNA, <<http://security.internet2.edu/fwna>>), is attempting to solve the same problem (see <<http://security.internet2.edu/fwna/minutes/NetAuth-FWNA-24-February-2005.html>> for additional background). More people want guest access, and Misra knows his organization must be responsive. "We currently have a guest access policy and are working on improving the application that delivers those accounts to members of the community," Misra said.

Table 3-11. Wireless Security Rate of Change, by Carnegie Class and Canada (N = 204)

Wireless Security Protection	DR	MA	BA	AA	Canada
40-bit Wired Equivalent Privacy (WEP)	-2.5%	93.9%	0.5%	-38.8%	35.1%
128-bit Wired Equivalent Privacy (WEP)	72.6%	-16.4%	53.4%	8.2%	20.0%
Extensible Authentication Protocol (EAP)	357.1%	363.3%	627.6%	26.3%	33.3%
Internet protocol virtual private network (IP VPN)	53.1%	68.7%	96.7%	59.3%	71.7%
Firewall	127.1%	52.5%	66.0%	108.6%	16.9%
Kerberos	72.6%	318.0%	15.4%	5.3%	1,010.0%
Remote authentication dial-in user service (RADIUS)	55.6%	43.1%	57.5%	5.3%	6.0%
Advanced Encryption Standard (AES)	1,735.7%	460.0%	22.7%	950.0%	200.0%
Wireless-vendor-supplied proprietary solution	51.7%	54.9%	122.4%	5.2%	35.1%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 3-12. Wireless Security Rate of Change, by Carnegie Class, from 2001 (N = 299) to 2005 (N = 413)

Wireless Security Protection	DR	MA	BA	AA
Remote authentication dial-in user service (RADIUS)	138.0%	179.5%	449.0%	141.4%
Firewall	207.0%	160.4%	376.0%	61.5%
Internet protocol virtual private network (IP VPN)	137.2%	276.7%	278.0%	3,730.0%
128-bit Wired Equivalent Privacy (WEP)	23.9%	-25.0%	3.5%	-14.8%
Kerberos	306.3%	510.0%	620.0%	317.5%
Wireless vendor supplied proprietary solution	220.0%	202.5%	132.7%	114.5%
40-bit Wired Equivalent Privacy (WEP)	137.8%	-23.8%	-11.9%	-7.2%
Extensible Authentication Protocol (EAP)	205.0%	330.0%	560.0%	242.5%

Note: Comparisons of changes between 2001 and 2005 are based on data from the 492 institutions that participated in the 2005 study and 299 institutions that participated in the 2001 study.

Table 3-13. Average Number of Wireless Strategies, by Carnegie Class and Canada (N = 446)

Institution Type	Number of Institutions	Mean	Std. Deviation
DR	120	4.03	1.95
MA	130	3.24	1.99
BA	87	3.28	1.95
AA	76	2.95	1.95
Canada	33	3.94	2.29

Identity Management

In his study of identity management, Ron Yanosky uses the Burton Group's definition: "The set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities." He further elaborates upon identity management (IdM) functions to include "establishing identity and user authentication and authorization. Supporting infrastructures for these core functions include enterprise directory services, reduced or single sign-on, automation of role- and privilege-based authorization, and creation of identity federations" (Yanosky, 2006, p. 23). We note that the data from this survey closely match Yanosky's data.

Access control and authentication have been called an arms race by the 2005 Cybersecurity Summit. Access control is a set of procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and limit access to a system's resources to only authorized persons, programs, processes, or other systems. It is not without controversy in the academic community, as it brings with it a loss of privacy. According to Steve Worona, director of the policy and networking program at EDUCAUSE, "There is no solution to this problem, just trade-offs."

Authentication is a method for confirming a user's credentials, often as a prerequisite to allowing access to a system's resources. We

asked our respondents what methods they use for authentication. Table 3-14 shows in rank order what is currently implemented, in progress, to be implemented within the next 12 months, and not under consideration.

Conventional passwords/PINs predominate (94.4 percent) and are, in general, the accepted methods. We found that 26.9 percent of the respondents use Kerberos. The other methods find significantly lower levels of use and are used mostly at doctoral institutions (see Table 3-15). And again we find that the doctoral institutions use these technologies at higher percentages across the board, with strong passwords, Kerberos, and one-time passwords being significantly higher.

The change between 2003 and 2005 is marginal for the 204 institutions in our comparison group. We note a 5 percent increase in Kerberos use and a 1.7 percent increase in biometrics. In 2005 we broke out PKI into four categories as opposed to one, making comparison difficult; but it appears that PKI has made little headway in two years.

The average number of authentication tools institutions in this study use is a mean of 2.1. Ninety percent of the respondents report using three or fewer of the tools in Table 3-14, and fewer than 3 percent use five or more. Only one institution used all 11.

We note that the 2005 CSI/FBI Computer Crime and Security Survey reported that 15 percent of their respondents had installed biometric tools, compared with 2.8 percent

Table 3-14. Authentication and Access Control Approaches Implemented (N = 492)

IT Security Approach	Already Implemented	Implementation in Progress	Will Implement within 12 Months	Not Planning to Implement within 12 Months	Don't Know
Conventional password/PIN	94.4%	0.0%	0.0%	4.5%	0.1%
Strong password	59.8%	12.8%	7.9%	15.9%	3.5%
Kerberos	26.9%	2.9%	4.2%	56.8%	9.1%
Secure ID-style one-time password	8.9%	2.8%	5.1%	74.7%	8.5%
Other multifactor authentication methods	8.1%	4.0%	7.0%	70.2%	10.6%
PKI certificate (software) without PIN	6.8%	1.3%	3.0%	78.5%	10.4%
PKI certificate (software) with PIN	5.1%	1.5%	2.5%	80.3%	10.1%
Biometric identification	2.8%	2.3%	4.0%	83.4%	7.4%
PKI hardware token with PIN	1.7%	1.7%	2.6%	83.6%	10.4%
PKI hardware token without PIN	0.9%	0.9%	1.3%	81.5%	10.8%

Table 3-15. Authentication and Access Control Implemented, by Carnegie Class and Canada (N = 446)

IT Security Approach	DR	MA	BA	AA	Canada
Conventional password/PIN	95.0%	93.8%	94.1%	89.3%	100.0%
Strong password	73.9%	53.1%	64.3%	45.9%	68.8%
Kerberos	41.9%	22.4%	16.7%	21.9%	38.7%
PKI certificate (software) without PIN	12.1%	3.2%	3.7%	1.4%	20.0%
PKI certificate (software) with PIN	7.7%	3.2%	3.7%	2.8%	6.7%
PKI hardware token without PIN	3.4%	0.0%	0.0%	0.0%	0.0%
PKI hardware token with PIN	2.6%	0.8%	2.4%	0.0%	0.0%
Secure ID-style one-time password	19.7%	2.4%	3.7%	5.4%	16.7%
Other multifactor authentication methods	11.9%	7.3%	7.2%	7.0%	13.3%
Biometric identification	4.3%	3.2%	3.6%	0.0%	3.4%

in our study. The other significant difference is less dependence on passwords and greater use of smart cards, PKI, and one-time password tokens by industry. This difference may be attributable to the diverse user population served by the higher education community. Corporate or government users are almost exclusively employees of the organization, making it easier and more cost-effective to deploy more advanced authentication methods to them. In contrast, a high percentage of the users on a higher education network are students, whose computers are not owned or managed by the institution. In addition, the higher education community has many “transient” users—students, part-time faculty, campus visitors—making it impractical to deploy methods such as hardware tokens or biometrics that require purchase, distribution, and training for additional hardware and software to function.

Nevertheless, Indiana University’s Mark Bruhn believes that authentication tools will become more prevalent in higher education. For example, keyboards will come out standard with thumb readers. If not keyboards, then some other commodity hardware with identification capabilities will become readily available, making the huge support burden of helping users manage passwords go away. Some USB device may also come along to support strong authentication, and directories will become more useful for maintaining IdM. Of course, such devices will raise new issues: stronger security is often intrusive and generally raises privacy concerns. For example, storing thumbprints on a central server rightly makes people nervous, especially given current data leaks.

Steve Worona at EDUCAUSE informs us that external demands to provide identity information may coerce higher education to make significant changes. Homeland Security Presidential Directive HSPD12 mandates standardized, high-assurance identification for

federal employees. Legislation under consideration would require higher education institutions to retain more information in case it is needed by law enforcement. “We are not the dog, we are the tail, and will have to be governed by society’s decisions,” said Worona. He predicts that it will be a rule rather than the exception that from an early age people will have a physical token to establish identity, real and virtual. People will thus arrive on campus with preestablished identity.

In the interim, Bruhn notes that password management has been strengthened. Three years ago, Indiana University had many disparate systems and kludgy ways of coordinating passwords. They have improved the quality of passwords and have moved from open source and homegrown software to Microsoft MIIIS and surrounding products to manage identity. Further, they have eliminated multiple identifiers at the enterprise level that individuals use, though departmental identifiers may still be in place. They have worked at discouraging users from acting as administrators for day-to-day activities on desktop systems. While IU will stay with username/password as the primary authentication method for the foreseeable future, passwords will become pass phrases, and minimum lengths will go from seven characters to 14 or so. Some key systems (HR, student, and financial) have cards for physical second-factor credentialing, but Bruhn doesn’t see this being a universal solution (currently about 10,000 of 120,000 users are supported this way). Indiana University is now among those looking at Shibboleth and InCommon.

Strategies to Reduce IT Security Vulnerability

We asked institutions what strategies they were using to reduce IT security vulnerability (see Table 3-16). We then rank ordered the strategies implemented. The most often used strategies were limiting protocols allowed

Table 3-16. Strategies to Reduce IT Security Vulnerability (N = 492)

Strategy	Already Implemented	Implementation in Progress	Will Implement within 12 Months	Not Planning to Implement within 12 Months	Don't Know
Limiting the types of protocols allowed through the firewall/router	87.1%	7.4%	1.4%	2.9%	1.2%
Restricting and eliminating access to servers and applications	79.6%	14.9%	1.6%	2.5%	1.4%
Timing-out access to specific applications after an idle period	77.0%	6.2%	2.7%	11.1%	3.1%
Instituting a recovery or backup plan in the case of disasters caused by natural events or by human acts	46.4%	30.8%	15.2%	6.2%	1.4%
Isolating or quarantining computers that do not meet minimum security requirements	45.3%	18.6%	19.1%	14.3%	2.7%
Installing closed desktop systems that don't allow user configuration changes	37.0%	15.0%	3.1%	39.2%	5.7%
Limiting the URLs allowed through the firewall	34.7%	5.6%	3.9%	50.6%	5.2%
Installing a software inventory system to watch for malicious software or program changes	16.4%	17.2%	12.5%	46.4%	7.4%
Using security devices (such as cards or biometric scanners) for authentication	14.0%	7.2%	10.7%	59.7%	8.3%

through the network firewall or router (87.1 percent), restricting or limiting access to servers and applications (79.6 percent), and timing-out access to applications after an idle period (77.0 percent). Little used were installing a software inventory system to watch for malicious program changes (16.4 percent) and security devices for personal authentication (14.0 percent). The latter two strategies and

limiting URLs through network firewalls were not under consideration by half or more of the respondents. Perhaps what is most disturbing in these data is that only 46.4 percent reported having a disaster recovery plan.

The average number of security strategies adopted by each institution is 4.30. There is little difference by Carnegie class or with Canadian respondents.

We looked to see where changes had taken place between 2003 and 2005 (see Table 3-17). The biggest change in terms of new adopters has been in limiting the types of protocols through the firewall/router (15.7 percent), timing-out access (11.0 percent), and restricting access to servers and applications (10.8 percent). With the exception of disaster recovery plans, we find that each technology has increased in use. The percentage of respondents reporting a disaster recovery plan is down 2.0 percent, a number we cannot explain. Note, too, that these changes are far less dramatic than what was reported earlier in this chapter. Approaches change quickly and strategies much less so!

Noteworthy, too, is that approaches used are similar in rank order (see Table 3-19).

The low growth rates also appear in Figure 3-3. Note that unlike growth and market penetration in earlier figures, high growth rates have not pushed these strategies into the high-market-penetration, high-rate-of-growth quadrant. Most of the strategies fall into two quadrants: high market penetration, low rate of growth; and low market penetration, low rate of growth.

Table 3-18 shows the strategies respondents are using, by Carnegie class. The conclusion to be drawn from this table is that, in general, doctoral institutions are less restrictive, with the exception of using security devices and software inventory systems. AA institutions are significantly more likely to use closed desktop systems (52.0 percent).

Table 3-17. Changes to Strategies to Reduce IT Security Vulnerability (N = 204)

Strategy	Percentage Used in 2005	Percentage Used in 2003	Percentage New Adopters	Rate of Change 2003–2005
Limiting the types of protocols allowed through the firewall/router	88.7%	73.0%	15.7%	21.5%
Restricting and eliminating access to servers and applications	80.9%	70.1%	10.8%	15.4%
Timing-out access to specific applications after an idle period	76.0%	65.0%	11.0%	16.9%
Instituting a recovery or backup plan in the case of disasters caused by natural events or by human acts	44.3%	46.3%	–2.0%	–4.3%
Limiting the URLs allowed through the firewall	29.1%	26.9%	2.2%	8.2%
Installing a software inventory system to watch for malicious software or program changes	17.7%	11.4%	6.3%	55.3%
Using security devices (such as cards or biometric scanners) for authentication	15.8%	12.3%	3.5%	28.5%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

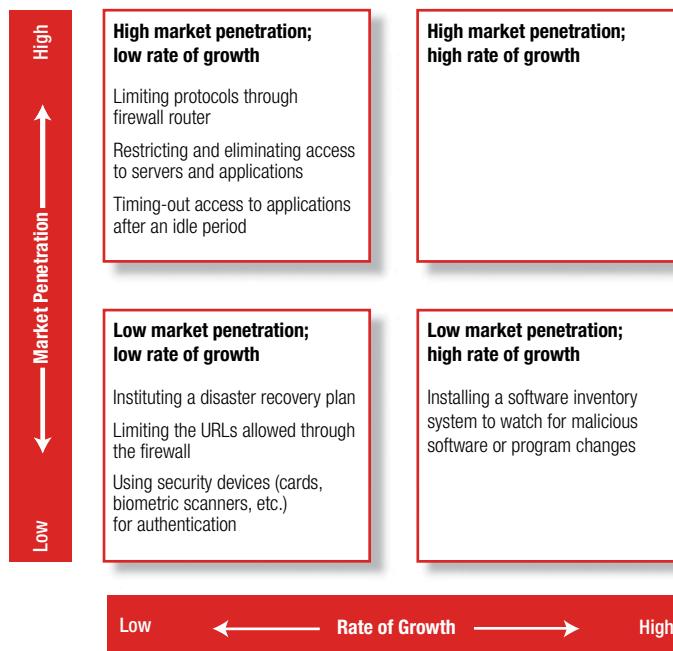


Figure 3-3.
Market Penetration and Growth Rate of Security Strategies, 2003 to 2005 (N = 204)

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 3-18. Strategies to Reduce IT Security Vulnerability, by Carnegie Class (N = 446)

Strategy	DR	MA	BA	AA	Canada
Limiting the types of protocols allowed through the firewall/router	82.5%	90.7%	88.4%	85.3%	87.9%
Limiting the URLs allowed through the firewall	21.0%	45.0%	28.9%	43.2%	30.3%
Restricting and eliminating access to servers and applications	67.5%	81.4%	87.2%	82.7%	81.8%
Timing-out access to specific applications after an idle period	70.8%	77.3%	76.5%	80.0%	81.8%
Using security devices (such as cards or biometric scanners) for authentication	19.3%	12.5%	13.3%	6.7%	21.2%
Installing a software inventory system to watch for malicious software or program changes	20.0%	13.3%	14.1%	13.3%	18.2%
Installing closed desktop systems that don't allow user configuration changes	22.5%	37.8%	36.0%	52.0%	51.5%
Instituting a recovery or backup plan in the case of disasters caused by natural events or by human acts	41.7%	55.0%	35.3%	51.4%	33.3%
Isolating or quarantining computers that do not meet minimum security requirements	45.8%	54.7%	52.3%	32.0%	45.5%

Note also the remarkably similar rank order of strategies used even while the percentage use of strategies used by the doctoral institutions is lower (see Table 3-19). This likely reflects the greater problem of decentralization at doctoral institutions. We also see a difference in limiting URLs through the firewall by doctoral institutions. When we view this strategy by FTE enrollments, the number is even more extreme, with 9.1 percent of respondents with FTE enrollment over 25,000 having already implemented limits on URLs through the firewall, versus over 40.0 percent by respondents with enrollments under 8,000.

Table 3-20 shows an unexplainable number of negative changes (reduced rates of usage), particularly for the doctoral institutions.

In summary, higher education is in the process of adopting more technologies to secure its vast information assets. But we found significant variation in patterns of adoption among Carnegie classes. When compared with the private and business sector, higher education lags in the installation of more advanced IT security technologies, but this may be due to different levels of risk, as noted earlier in this chapter, as well as to the diverse populations being served.

Table 3-19. Rank Order of Strategies to Reduce IT Security Vulnerability, by Carnegie Class (N = 446)

Strategy	DR	MA	BA	AA	Canada
Limiting the types of protocols allowed through the firewall/router	1	1	1	1	1
Restricting and eliminating access to servers and applications	3	2	2	2	2
Timing-out access to specific applications after an idle period	2	3	3	3	3
Installing closed desktop systems that don't allow user configuration changes	6	7	5	4	4
Isolating or quarantining computers that do not meet minimum security requirements	4	5	4	7	5
Instituting a recovery or backup plan in the case of disasters caused by natural events or by human acts	5	4	6	5	6
Limiting the URLs allowed through the firewall	7	6	7	6	7
Using security devices (such as cards or biometric scanners) for authentication	9	9	9	9	8
Installing a software inventory system to watch for malicious software or program changes	8	8	8	8	9

Table 3-20. Rate of Change of Strategies to Reduce IT Security Vulnerability, by Carnegie Class, 2003 to 2005 (N = 204)

Strategy	DR	MA	BA	AA	Canada
Limiting the types of protocols allowed through the firewall	35.3%	25.0%	3.1%	30.8%	0.0%
Limiting the URLs allowed through the firewall	14.6%	6.0%	20.7%	14.2%	28.6%
Restricting and eliminating access to servers and applications	3.5%	24.1%	15.4%	79.0%	14.3%
Timing-out access to specific applications after an idle period	-21.0%	13.6%	-38.4%	149.3%	50.0%
Using security devices (such as cards or biometric scanners) for authentication	-14.7%	27.7%	0.0%	120.2%	74.7%
Installing a software inventory system to watch for malicious software or program changes	21.7%	153.3%	154.7%	0.0%	4.9%
Installing closed desktop systems that don't allow user configuration changes	48.1%	0.0%	33.5%	101.0%	1,720.0%
Instituting a recovery or backup plan in the case of disasters caused by natural events or by human acts	-28.9%	27.8%	9.3%	50.0%	0.0%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.