

SOME SECURITY AREAS INTERNET2 COULD WORK ON

Security Area	Nutshell Description	Why Is This A Worthy Area?	How Bad Is It?	Key Technologies	Key Commercial/ Technical Partners
1. Spam	Unwanted Email, IM, Web and VoIP Traffic	Messaging and The Web Remain The Net's "Killer Apps"	Over 90% of All Email is Now Unwanted Traffic	SpamAssassin, DNS and URI Block Lists, SPF, DKIM	Messaging Anti-Abuse Working Group (MAAWG)
2. Malware	Viruses, Worms, Trojan Horses, Spyware, Other Malicious Software	Malware Undercuts The Security of The PCs Used For Everything Else	Malware Is Being Released Faster Than Vendors Can Update Antivirus Signatures	Antivirus Software, Heuristic Detection, Sandboxing, Secure Coding Practices	The Antivirus Community; Antivirus Vendors
3. Phishing	Tricking Users Into Revealing Secret Account Passwords	Phishing Reduces Confidence in E-Commerce Security	Some Months, Over 50K Unique Phish Sites Get Reported	Browser Alerts, URI Block Lists, EV Certs, Registrar Audits	Anti-Phishing Working Group (APWG), ICANN
4. Distributed Denial of Service (DDoS) Attacks	Connections Get Swamped With Large Floods of Traffic	DDoS Is The Most Worrisome Security Issue for Engineers	DDoS Attacks Have Taken Entire Countries Offline	Real Time Black Hole Communities, Hop-by-Hop Traceback	Arbor Networks
5. Encryption, Sniffing and Privacy	Eavesdropping On Sensitive Info Stored Or Sent Over the Net	Sniffed Passwords ==> Breaches; PII Breaches ==> Firing	Virtually All Networks May Be Subject To Monitoring	SSL, SSH, WPA2, PGP, VPN, Whole Disk Encryption	IDS Suppliers (e.g., Snort, Bro); PII Scanning Vendors
6. Replacing Traditional Passwords	Passwords Are Too Easy For Badguys To Sniff, Guess or Crack	Passwords Are Used By Virtually All Online Services	Short (<8 character) Passwords Can Be Cracked in <1 Week	Two Factor Auth: Crypto Tokens, Biometrics; Wallets	Two Factor Authentication Vendors
7. Firewalls, Middleboxes and End-to-End Transparency	Boxes Added To The Network To Protect Systems Break Legitimate Applications	Not Much Point To Having A Network If Legitimate Applications Can't Be Run	Estimates Are That 97% of All Sites Now Use Firewalls	Encryption, Tunneling, Circuit-Based Networks	Jericho Forum
8. IPv6 and Security	Many Hardware Network Security Appliances Don't Know About IPv6	IPv6 Deployment Will Be Stalled Until Security Appliances Become IPv6 Aware	We'll Be *OUT* of IPv4 Addresses In <3 Years, So We Can't Wait To Get IPv6 Deployed	Vendor Issue	Hardware Security Appliance Vendors
9. Domain Names, IP Addresses, DNS and DNSSEC	Translation of Names to IP Addresses Is Untrustworthy	All Network Apps Trust DNS To Take Users to Sites	The Entire Internet Will Have to Upgrade Its Name Servers	DNSSEC, Disabling Open Recursion, Patch Nameservers	DNS-OARC, DHS, ARIN, ICANN, Shinkuru
10. Switching and Routing Security (Including Securing BGP)	Network Addresses Can Be Hijacked And Traffic Misrouted/ Compromised	Untrustworthy Routing/Switching Can Take Entire Sites Offline	This Area Is Still Virtually A Green Field Due to Other Security Concerns	S*BGP; Layer 2 Switching Security Measures; ARP Monitoring	RouteViews, DHS
11. FWNA/Netauth Wireless Net Access	Wireless Net Access (While Visiting A Participating Site) Via Home University Username/Password	University Visitors Are Currently Accomodated Via Non-Scalable Ad Hoc Means (Or Not At All)	84% Of Respondents to a 2007 Survey Offer Guest Access, But With Little Commonality of Method	Shibboleth, 802.1X, SAML, NAC, Eduroam, InCommon	ProtectNetwork

12. REN-ISAC Incident Handling & Trust Community	When University Systems Get Hacked, REN-ISAC Notifies Appropriate Folks	Compromised Systems Pose An Ongoing Threat Until Remediated	Most Internet2 University Members Participate In The REN-ISAC	Information Sharing Partnerships; Dark Space Telescope	Indiana University, LSU, Infragard
13. Development & Distribution of Operational Security Tools	The R&E University Community Writes Useful Security Programs Which Can Be Shared	Providing A Home For Open Source Tools Leverages The Communities Intellectual Property	One Tool Searches For PII; PII Breaches Are One Of The Most Dreaded Information Security Incidents	Cornell Spider Is The First Example of Such A Tool	Cornell University
14. Mobile Devices	Wireless Mobile Devices Can Pose Unique Network Security and Device Encryption Challenges	The iPhone (And Kin) Have Generated A Tremendous Level of Popular Interest	1.15 BILLION Cell Phones Were Sold Worldwide in 2007	Whole Device Encryption, Network Encryption (Sometimes 3rd Party Solutions)	Cellular Carriers and Wireless Providers
15. Disaster Planning and Recovery	Planning To Cope With Data Center Fires, Hurricanes And Other Campus Threats	Some Disasters (Such as Katrina or 9/11) Can Jeopardize Long Term Campus Survivability	Less Than 60% of Higher Ed Sites Have Disaster Recovery Plans	Offsite/Hot Site Replication; Emergency Notification Systems	Educause
16. Convening Senior Campus Leadership; Campus Expectations Task Force	Providing a Forum For University Leadership Engagement, Understanding, and Inter-site Comparison	Without The Support of Senior Leaders, It Is Hard For Security Programs To Succeed	Senior Campus Leaders May Not Have Capacity To Take On Additional High Priority Issues	N/A	Educause
17. Security Technology Evangelism and Leadership	Identifying and Publicizing the Most Pressing IT Security Issues Schools Face	Many Issues -- If You Miss or Mistakenly Focus On the Wrong Ones, You Lose...	Users May Feel Overwhelmed By Emerging Threat Info If Delivery Isn't Properly Phased	N/A	Educause
18. Security Policies	A Growing Body Of Laws, Regulations, Compliance Requirements and Policies All Impact Operational Security	One Example: PCI DSS Is Driving Many Campus Network Architectures; C.F., Network Neutrality, CALEA, DMCA, etc.	Deficient IT Policies Can Enable Risk Free Exploitation of Technical Security Vulnerability	N/A	ICPL, Educause
19. Engaging Standards Bodies (IETF, etc.) Regarding Security Issues	Some Security Issues Exist Which Can Only Be Fixed At the Protocol Level, And That's An IETF Thing	Participation In The IETF Process Gives Higher Education A Chance to Influence Emerging Protocols	Based On Informal Polls, Participation In IETF By Higher Education Is Currently Quite Low	N/A	Educause, IETF, ISOC, ICANN
20. Management/Security Support of Distributed Servers	Departments Or Other University or College Subunits May Operate Their Own Servers, But Have Limited System Support Resources	Distributed Servers May Have PII Data Or Critical Network-Exposed Services, Yet May Be Unpatched Or Otherwise Vulnerable	The Degree of Centralization/Decentralization Can Vary Substantially From Site to Site	TBD	TBD

Notes:

- This Chart Only Includes the Most Urgent of Issues; Additional Important Security Issues Also Exist Which Exceed Available Capacity
- Topics Are NOT Listed In Priority Order
- For Some Security Topics, Internet2 Will Be A Supporting Partner Rather Than the Lead For That Area