

# Applied Security Visualization

## Color Gallery

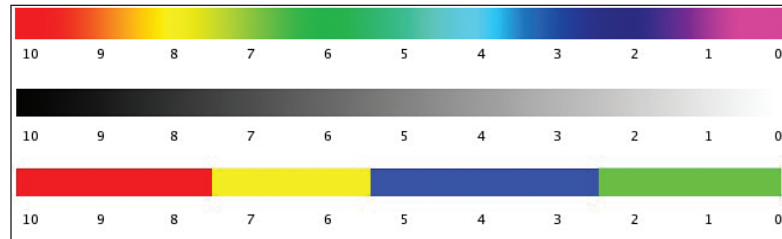


Figure 3-1

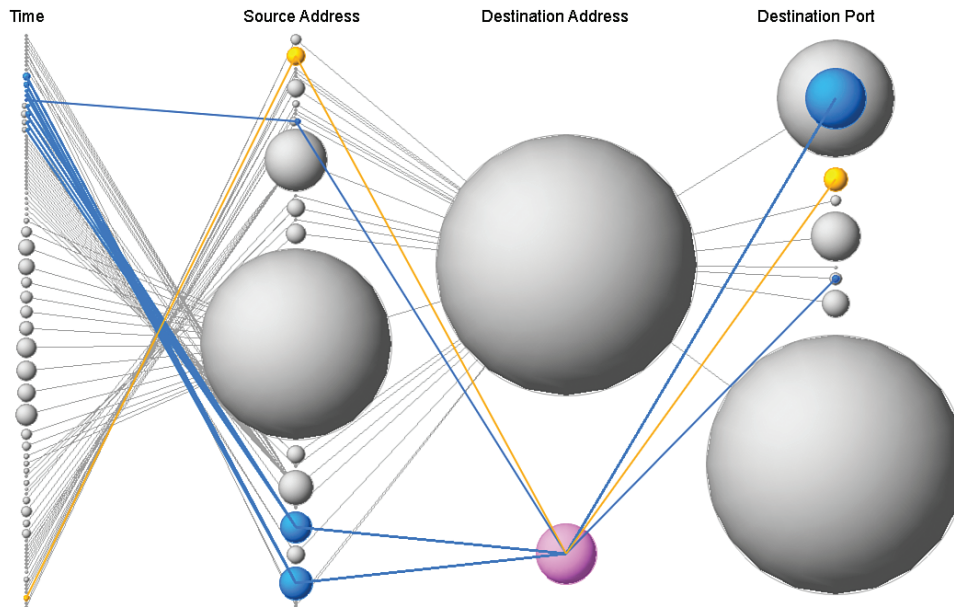


Figure 3-17

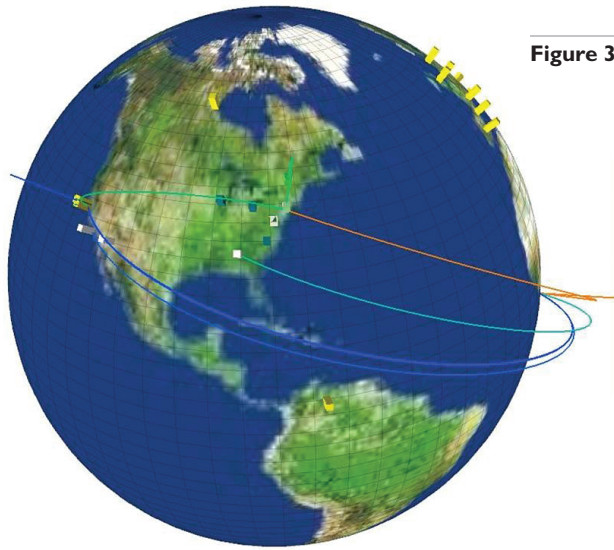


Figure 3-27

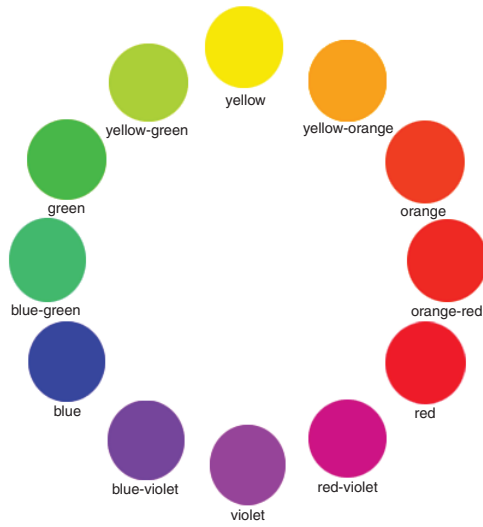


Figure 4-10

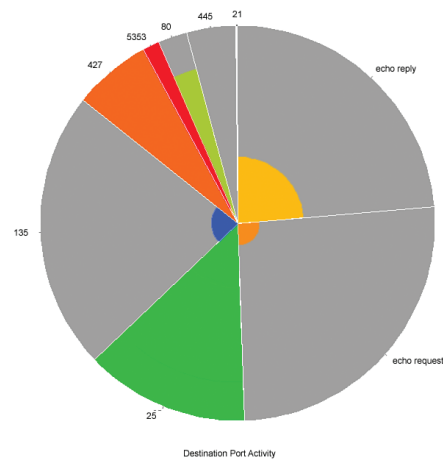
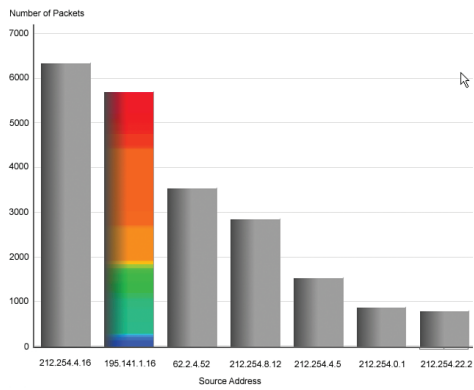


Figure 3-39

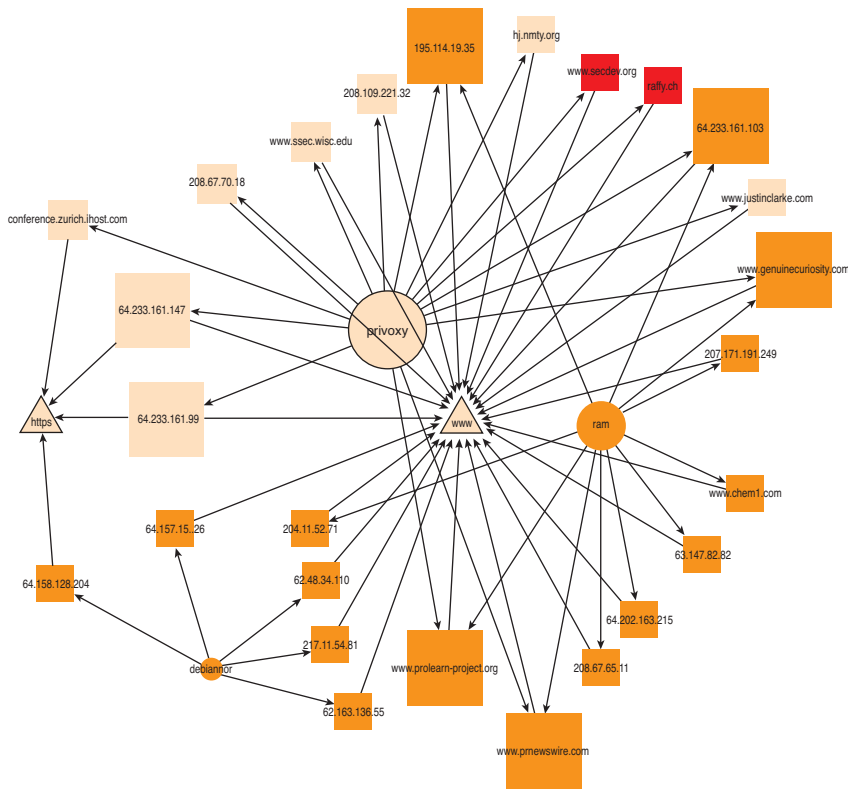


Figure 4-11

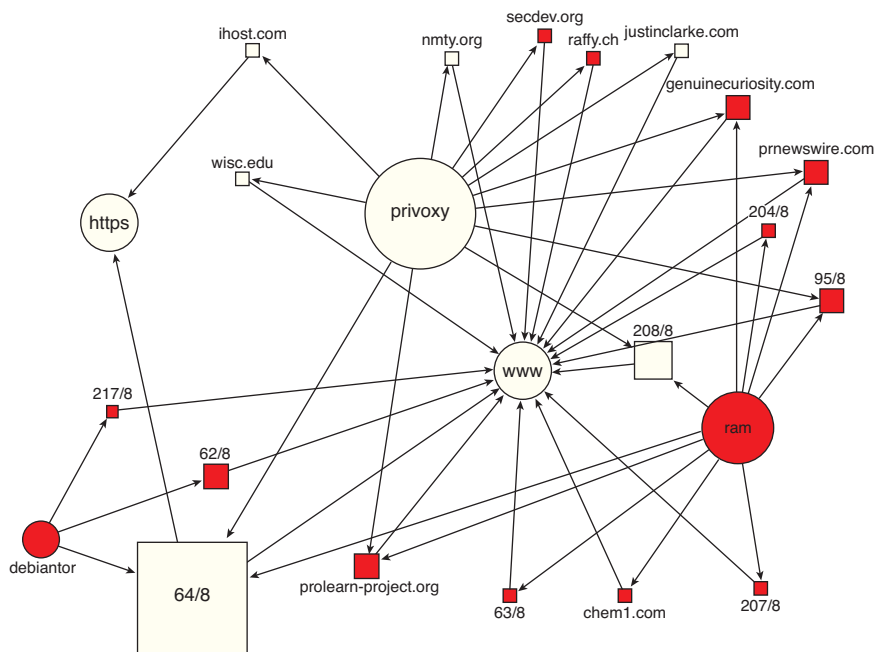


Figure 4-12

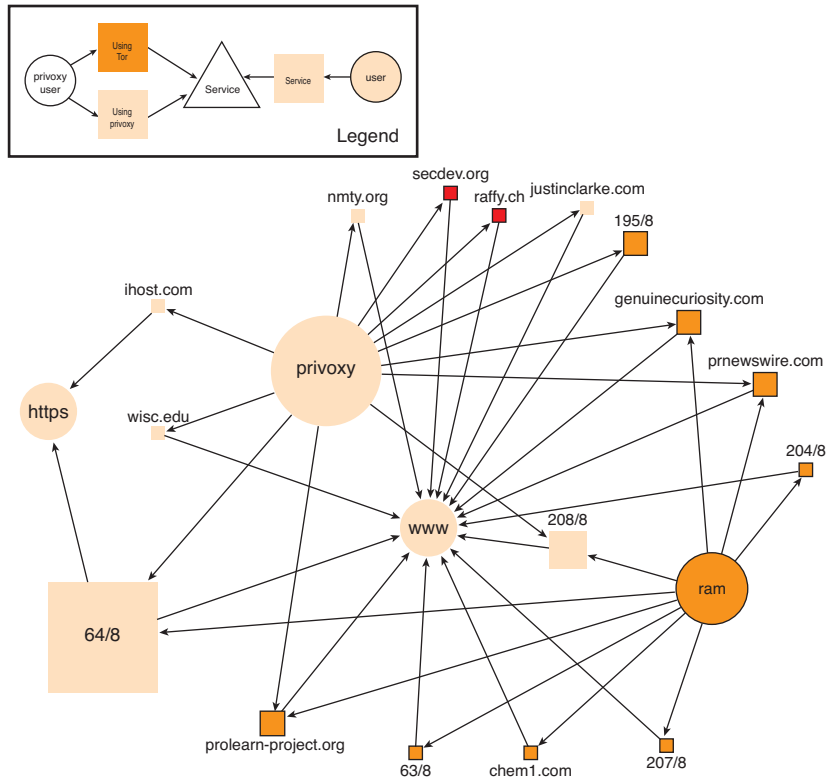


Figure 4-15

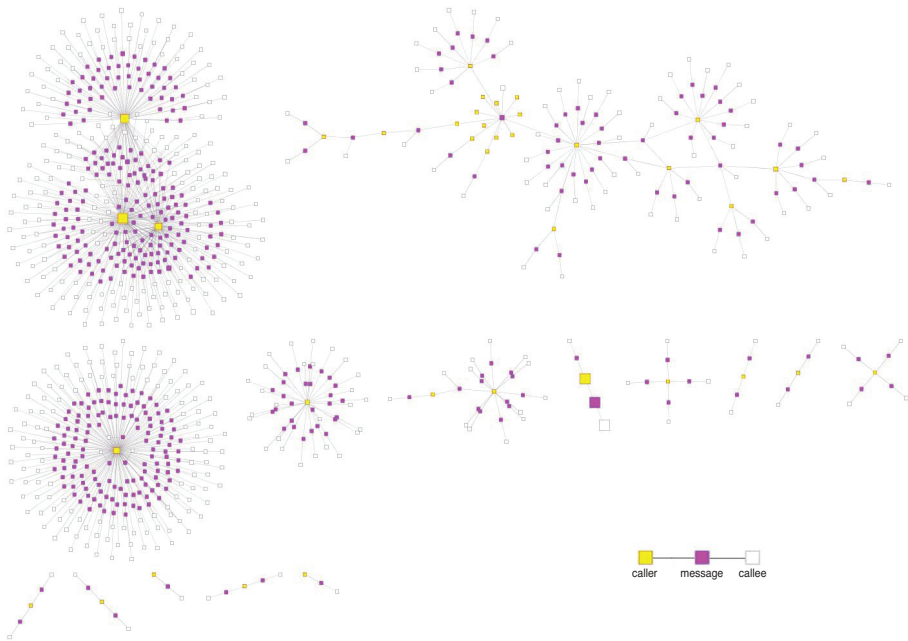


Figure 6-7

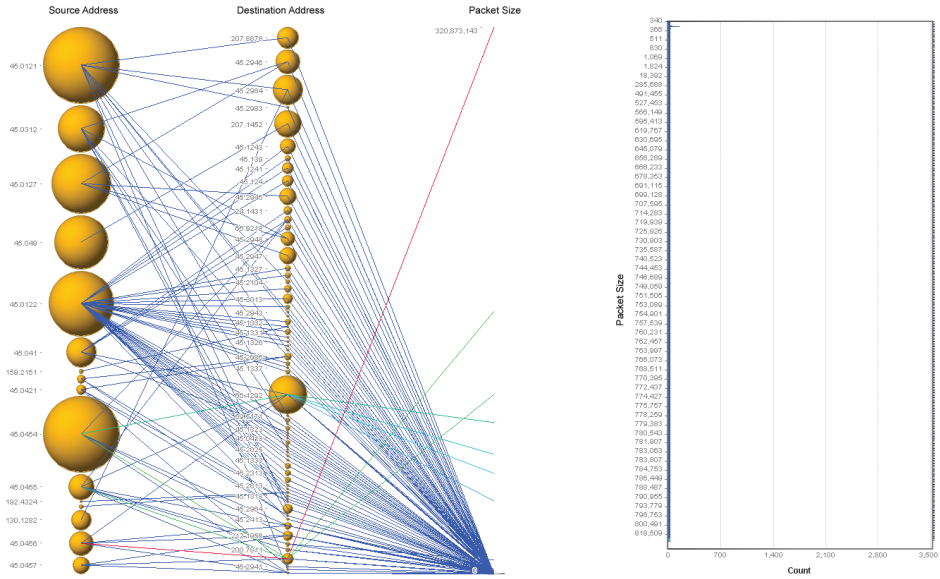


Figure 6-12

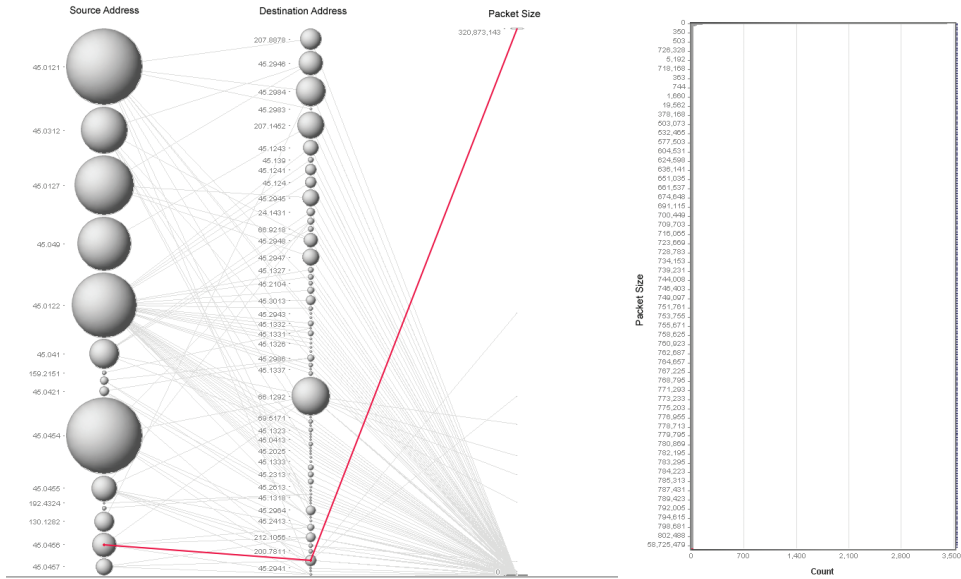


Figure 6-13

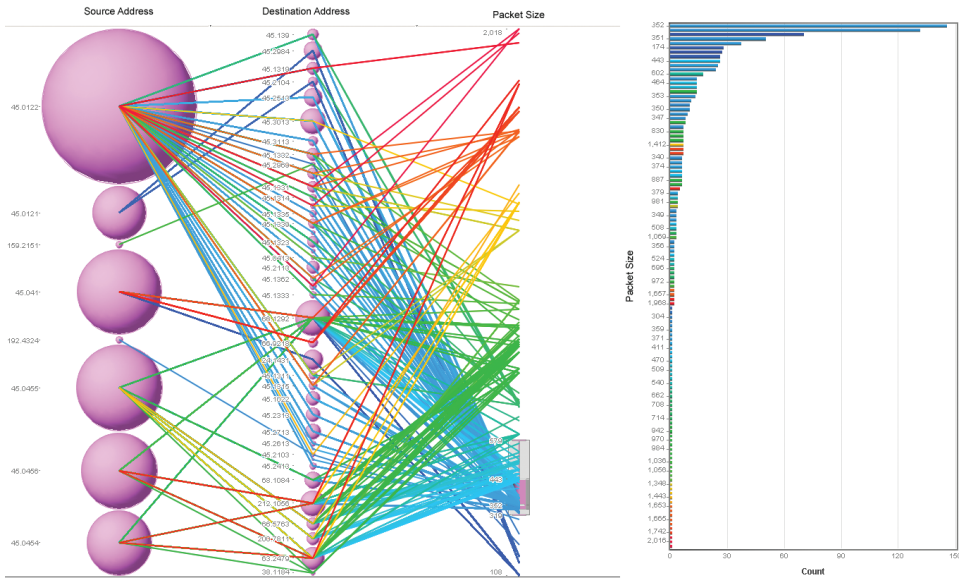


Figure 6-16

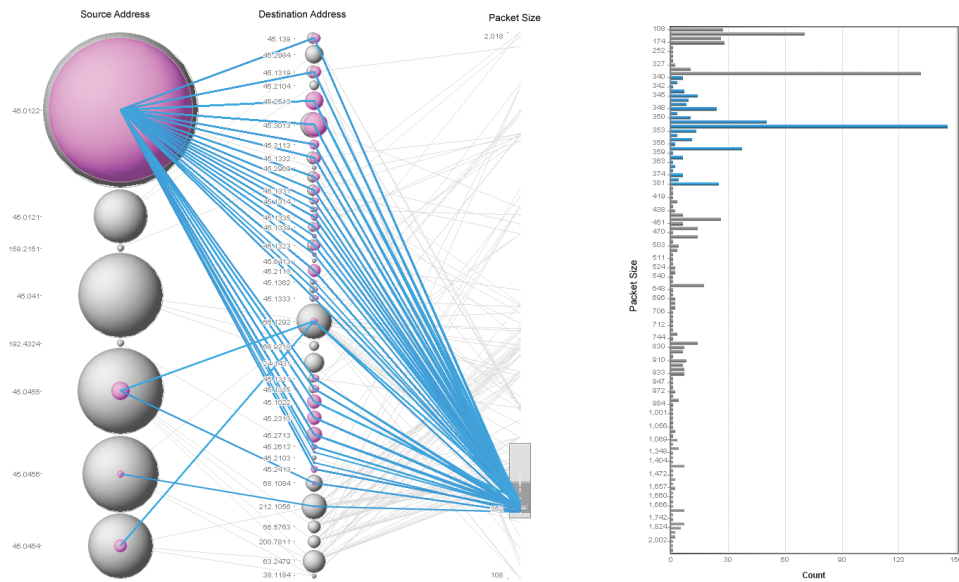


Figure 6-17

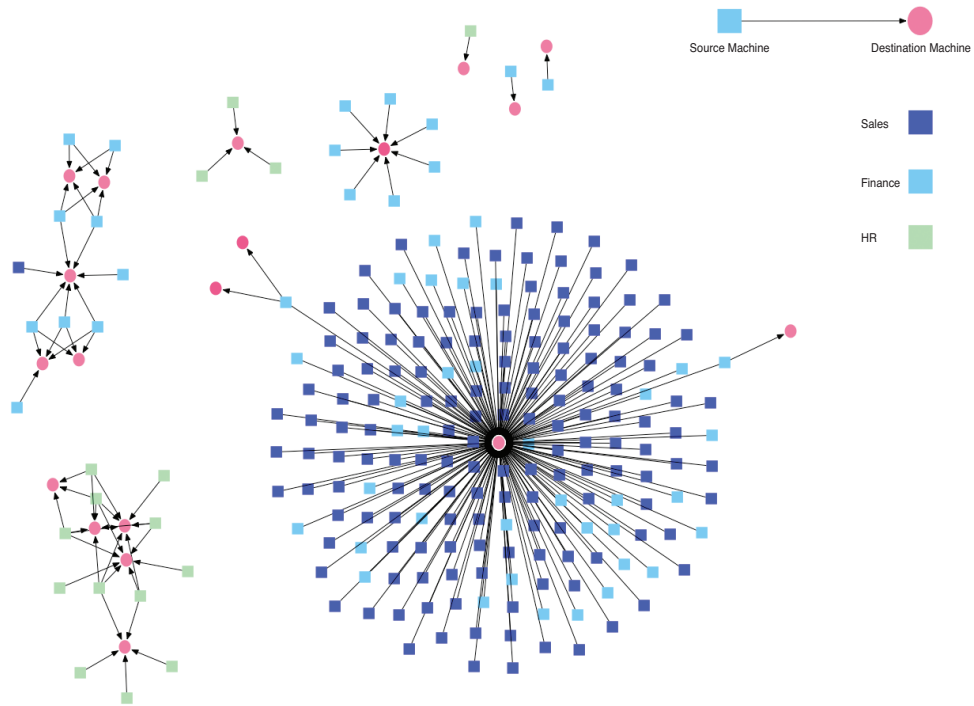


Figure 6-18

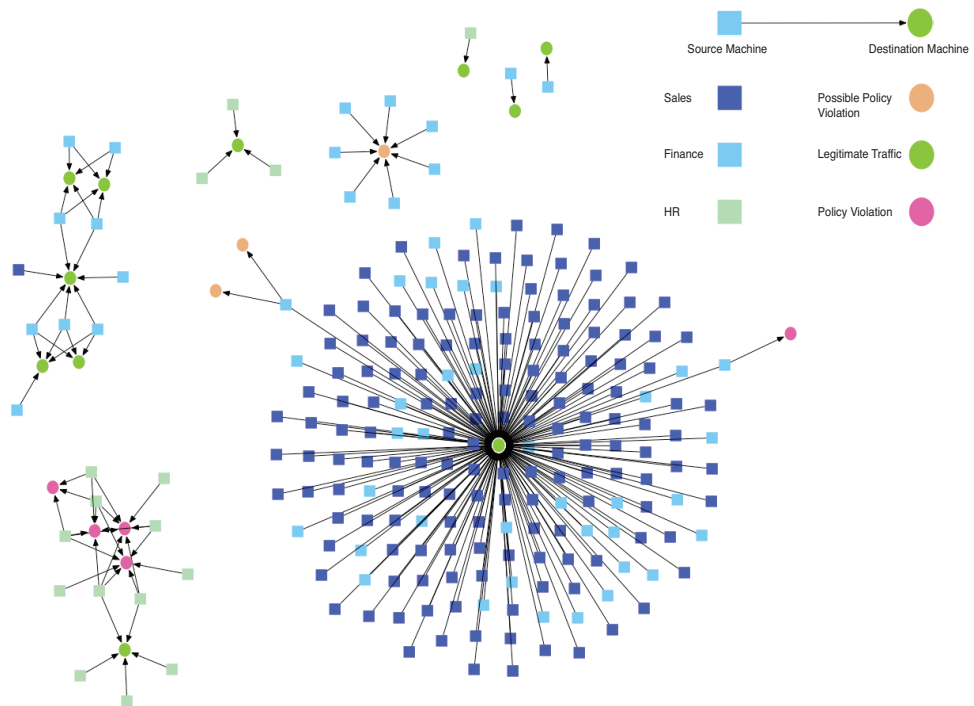


Figure 6-19

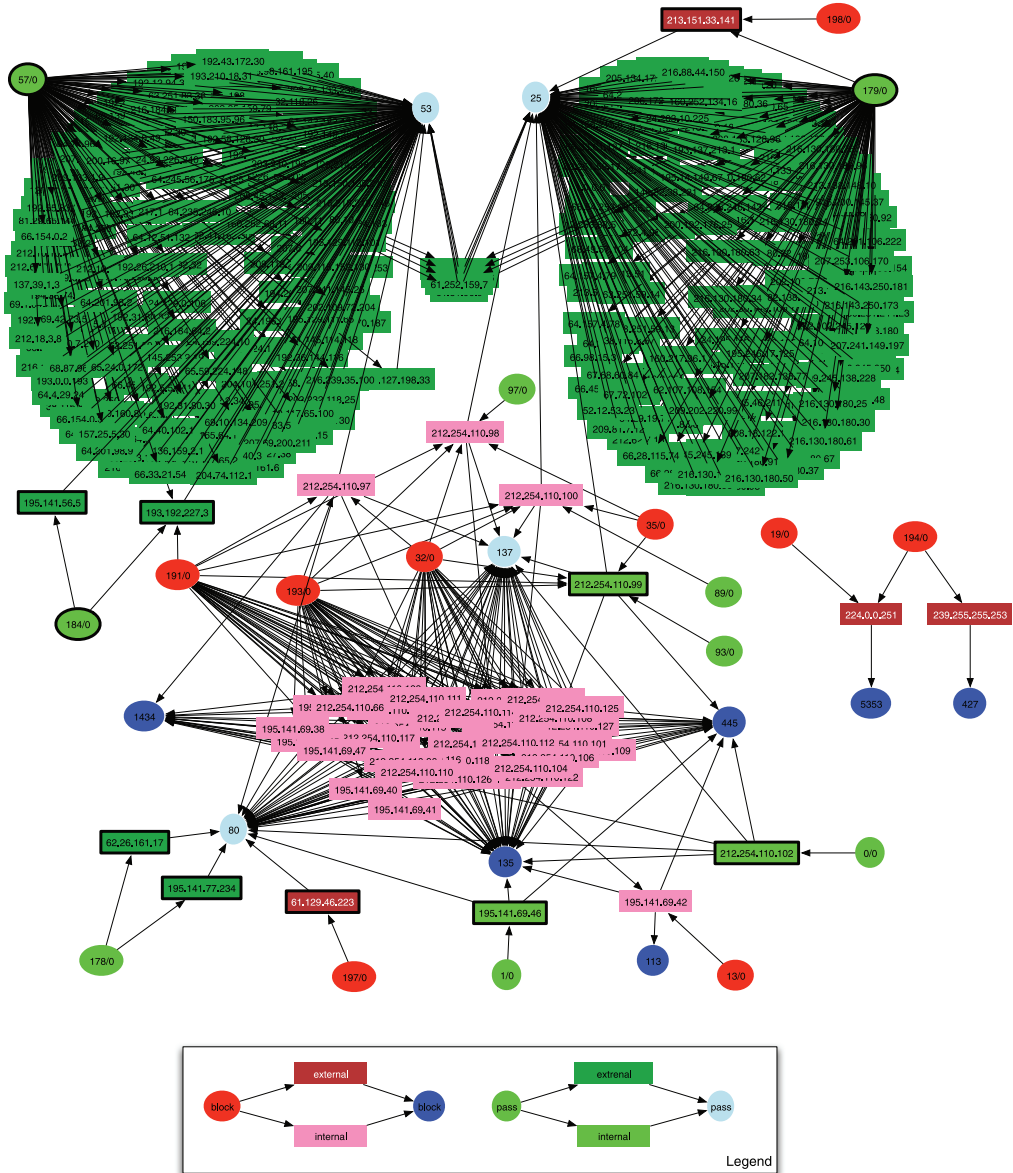


Figure 6-24



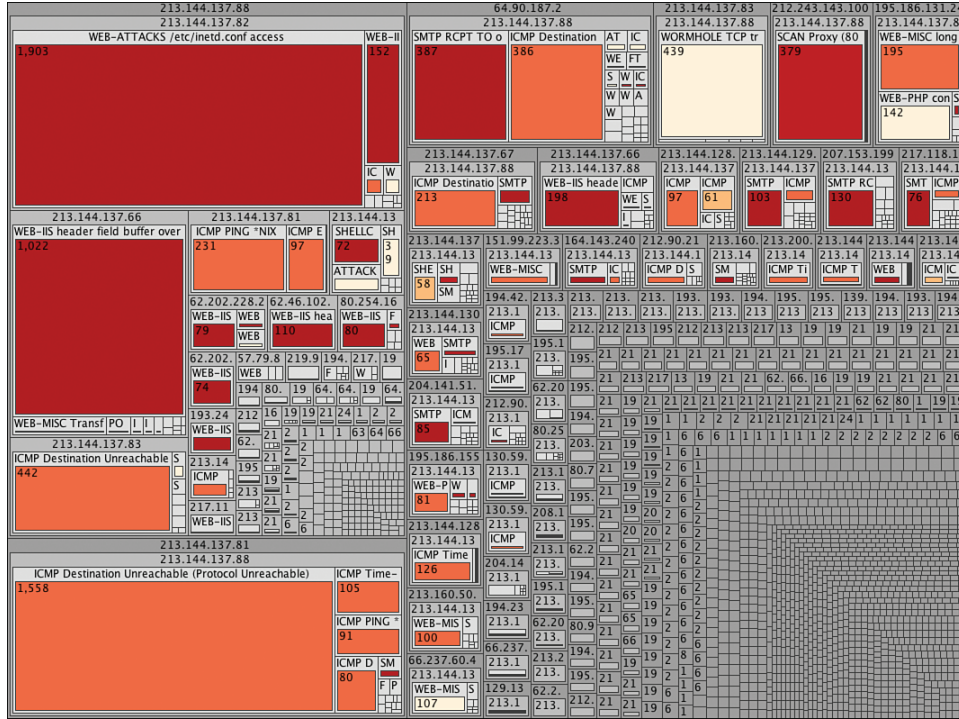


Figure 6-26

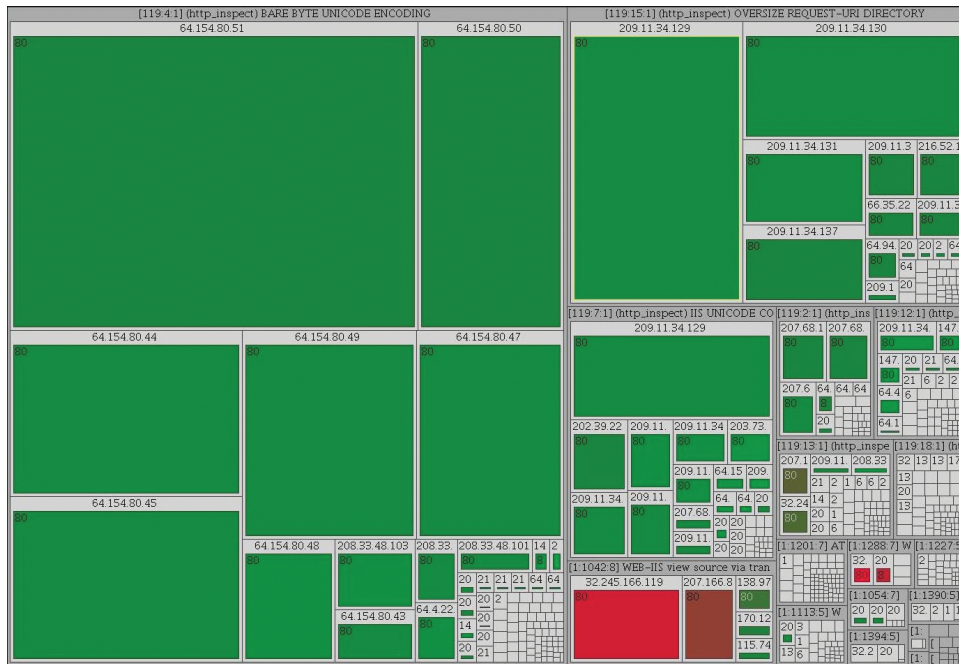


Figure 6-27





Control Objectives									
<b>User Account Management</b> <b>Access Management</b> Use identification to allow access to IT computing Use authorization mechanisms to allow access to IT computing Secure online access to data Implement access control for dial-up connections Establish least privilege access to data				<b>Establish firewall configuration standards</b> <b>Change Management</b> Approving changes to firewall configuration Current network diagram Monitor configuration standards for firewalls Testing changes to firewall configuration Review of firewall rule sets Monitor configuration standards for routers				<b>External Net</b> Approving external network connections Testing external network connections	
<b>New Accounts</b> Procedures for requesting user accounts Procedures for issuing user accounts		<b>Review</b> Management Review of User Accounts Management Confirmation of access rights Comparison of resources with recorded accountability		<b>Requirements</b> Requirements for a firewall at each Internet connection Requirements for a firewall between any DMZ and the Intranet		<b>Justification</b> List of services/ports necessary for business Justification and documentation for any available protocols		<b>Access Control Description</b>	
<b>Third Party</b> Define third-party		<b>Change Control</b> Enforce regular password changes		<b>Exceptions</b> Allow users to report unusual activity		<b>Surveillance</b> Security activity should be logged		<b>Firewall configuration Configuration</b> Deny all traffic from "untrusted" networks/hosts Allow Web protocols System administration protocols Other protocols required by the business Deny connections between publicly accessible Restricting inbound Internet traffic to DMZ	

Figure 7-6



Figure 8-6

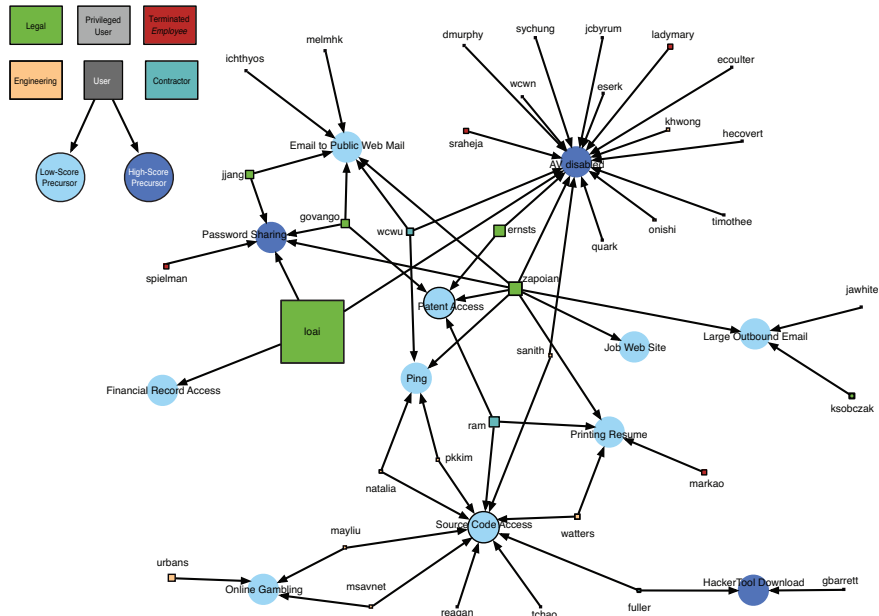


Figure 8-16

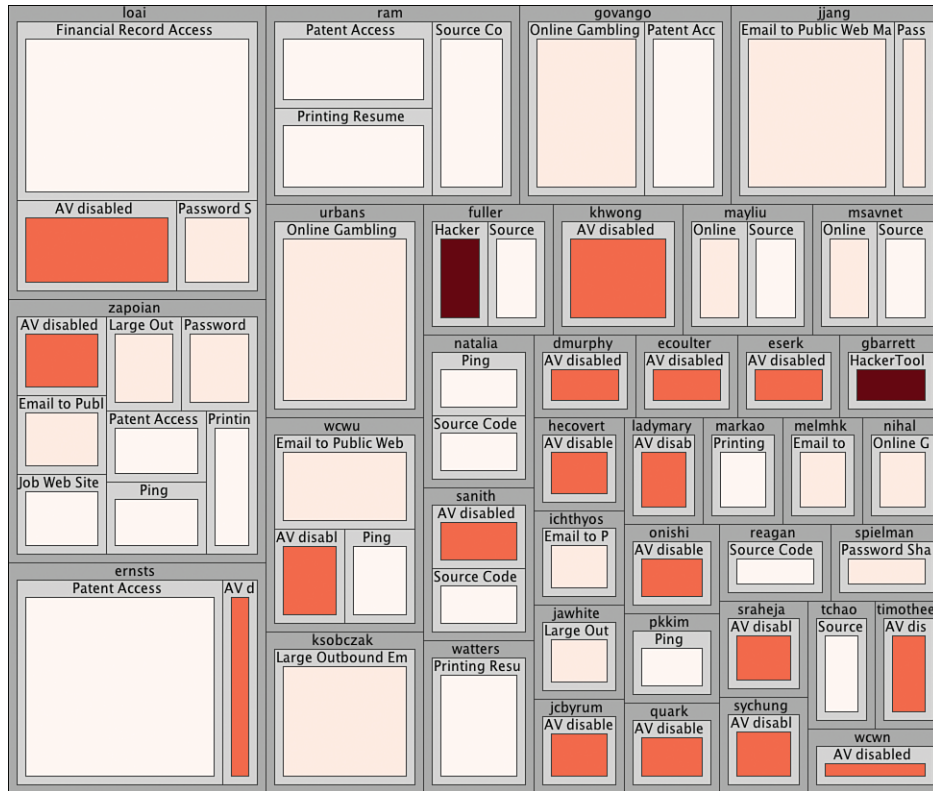


Figure 8-17



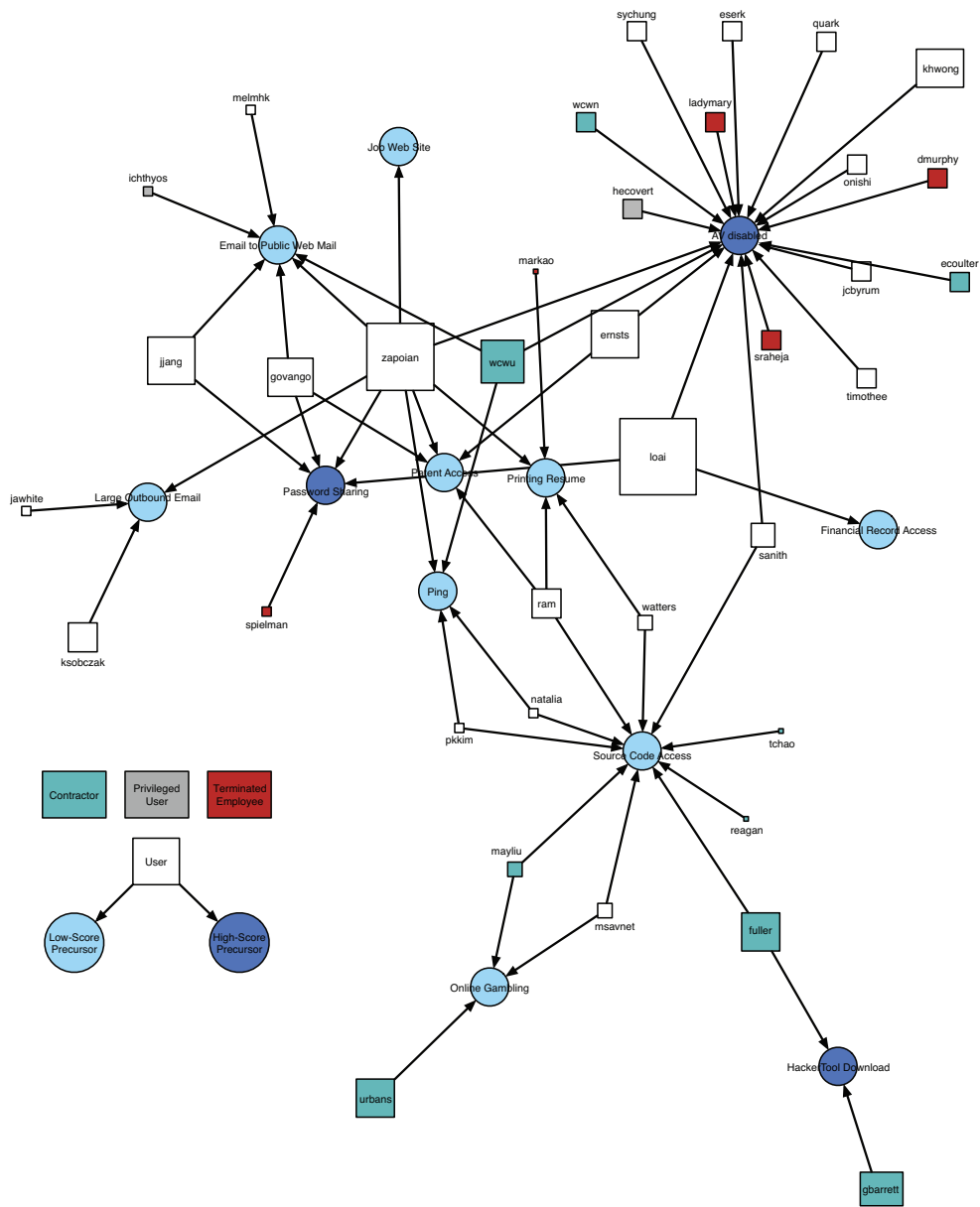


Figure 8-23

NONE				Contractor							
zapolan Minimal		Setup		loai Minimal		sanith Setup		fuller Malicious		gbarrett Malicious	
Email to Public Web Mail	Large Outbound Email	Patent Access	Ping	Financial Record Access	Password Sharing	AV disabled	Source Code Access	Hacker Tool Download	Source Code Access	Hacker Tool Download	
Job Web Site	Password Sharing	Printing Resume		Setup		Source Code Access	Source Code Access				
govango Minimal		khwong Setup		ladymary Setup		onishi Setup		wcwu Minimal		wcnw Setup	
Email to Public Web Mail	Patent Access	AV disabled		AV disabled		AV disabled		Email to Public Web Mail	AV disabled	AV disabled	
Password Sharing									Ping		
eserk Setup		quark Minimal		msavnet Minimal		ram Minimal		ecoulter Setup		mayliu Minimal	
AV disabled		AV disabled		Online Gambling	Source Code Access	Patent Access	Printin g	Source Code Access	AV disabled	Source Code Access	reagan Minimal
										Online Gambling	Source Code Access
jcbryum Setup		sychung Setup		jawhite Minimal		natalia Minimal		pkkim Minimal		tchao Minimal	
AV disabled		AV disabled		Large Outbound Email	Ping	Ping	Ping	Terminated		Privileged	
								dmurphy Setup		hecovert User Setup	
				ksobczak Minimal		Source Code Access		AV disabled		AV disabled	
				Large Outbound Email		Source Code Access		spielman Minimal		Password Sharing	
jjang Minimal		timothee Setup		watters Minimal		ernsts Setup		sraheja Setup		markao Minimal	
Email to Public Web Mail	Password Sharing	AV disabled		Printing Resume	AV disabled	Setup	Setup	AV disabled	AV disabled	Minimal Printing Resume	ichthos User Privileged User
				Email to Public Web Mail	Source Code Access	Minimal Patent Access	Minimal Patent Access				Email to Public Web Mail

Figure 8-24