September 2016 (Vol. 5; Issue 9)



Very few traditional government IT or defense

contractors competed in DARPA's Cyber Grand

Challenge and those that did fared poorly

In a similar vein as bake-offs, we have written many

times before about the value of bug bounties and their

effectiveness. The primary difference is that while bake-

offs are best for underlying components, bug bounties

can help identify weaknesses that result from the combi-

nation of secure components in a system. To mitigate the

potentially significant cost to initiate bug bounty efforts,

many firms are turning to outsourced platforms to man-

age their programs and responsible disclosures. From

Top 15 Products	Pwning DEF CON 24						
with Known Vulnerabilities	 The pervasive use of networking in the office and home has opened up numerous – and ever-increasing – security holes The market to secure the IoT is wide-open, but the burden of proof is higher than ever before and third party IV&V is required 						
1. Google Android Operating System	While individual components comprising IoT products may be secure, their amalgamation While individual components comprising IoT products may be secure, their amalgamation Next-gen hacking will be conducted by autonomous machines, not humans; expect vulnera-						

- 385 vulnerabilities 2. Debian Linux **Operating System** 278 vulnerabilities
- 3. Canonical Ubuntu Linux **Operating System** 238 vulnerabilities
- 4. Adobe Flash Player Application 226 vulnerabilities
- 5. Novell Leap **Operating System** 217 vulnerabilities
- 6. Novell OpenSuSE **Operating System** 216 vulnerabilities
- 7. Apple Mac OS X **Operating System** 166 vulnerabilities
- 8. Adobe Acrobat Reader Dc **Application** 152 vulnerabilities
- 9. Adobe Acrobat DC Application 152 vulnerabilities
- 10. Linux Kernel **Operating System** 151 vulnerabilities
- 11. Adobe Acrobat Application 149 vulnerabilities
- 12. Google Chrome **Application** 149 vulnerabilities
- 13. Adobe Reader Application 129 vulnerabilities
- 14. Apple iPhone **Operating System** 118 vulnerabilities
- 15. Mozilla Firefox Application 114 vulnerabilities

1751 Pinnacle Drive McLean, VA 22102 wolfdenassociates.com

1	The pervasive use of networking in the office and home has opened up numerous – and ever-increasing – security holes	The market to secure the IoT is we the burden of proof is higher that and third party IV&V is required
i	While individual components comprising IoT products may be secure, their amalgamation is often quite vulnerable	Next-gen hacking will be conduct mous machines, not humans; ex bility identification rates to soar

100 We are just seeing the tip of the IoT threat iceberg and extensive investment in training and testing is required to avoid disaster

Wall of Sheep

hospital

Since we wrote in August 2014 about how to protect yourself on the Cyber Serengeti, the stakes have gotten higher, the adversaries have gotten fiercer, and we are far more vulnerable. With the growth of the Internet of Things (IoT), there are more weak points than ever, providing attackers with nearly limitless possibilities for network entry and lateral movement, and all of us are now unwitting sheep. While competing in the IoT ethical hacking challenge at DEF CON 24, we generated hacks to lock your home thermostat, to disable your home network, and to remote

0

Source: Wolf Den Analysis

wheelchairs.

Within the IoT, we are

seeing a resurgence of

old-school hacks that es-

chew advanced memory

manipulation techniques,

instead deploying inse-

cure maintenance inter-

faces that allow arbitrary

In a world where security

is a requirement, but for-

mal definitions of "Secu-

rity" are scarce, it is

Rick T.

(703) 638-5924

Rick@wolfdenassociates.

code execution.

Get Baked

to disat ntrol mo	ole you otorized	r hur d are	nble be now ເ	eginnin used b	igs at e y tech	mergi giants	ng players, these platforms s including Adobe, Twitter,			
Tin	ne to Expl		SurveyMonkey, and Uber							
Mot	orola Focus		to manage "white hat" freelance programs. By							
	Asus AC66									
TF	LINK TL-10	43ND Wire	eless Route	r			outsourcing bug boun			
	D-LI	NK DIR-86	5L							
Hello Baby Monitor TCP Connected Smart LED Light Bulb Belkin N300 Wireless Router							ties, companies get trusted third-party sub-			
									missions and payout	
							Netgea	ır ReadyNas	Network A	
Pogo	plug Mobile	Wireless	Backup De	vice			inanagement, with bet-			
Seagate	Disk Statio	n Network	Attached S	torage			ter results and lower to-			
Western Di	gital Disk Sta		tal cost of ownership.							
	Belkin N9									
Contro	4 HC-250 Ho	ome Theat	er Control S	ystem						
50	75	100	125	150	175	200	I NIS YEAR AT DEF CON 24,			
	to disab ntrol mo Tin Mote Tr Tr Netgea Pogo Seagate Western Dip Control	to disable you ntrol motorized Time to Expl Motorola Focus Asus ACG TP LINK TL-100 TCP Connecte Belkin N33 Netgear ReadyNas Pogoplug Mobile Seagate Disk Station Western Digital Disk Stat	to disable your hun ntrol motorized are Time to Exploit Varia Motorola Focus 73 Outdoo Asus AC66u Wireles TP LINK TL-1043ND Wire BUINK TL-1043ND Wireles D-LINK DIR-86 Hello Baby Mon TCP Connected SmartLE Belkin N300 Wireles Netgear ReadyNas Network A Pogoplug Mobile Wireless Seagate Disk Station Network Western Digital Disk Station Network Belkin N300 Wireles Control4 HC-250 Home Theat	to disable your humble be ntrol motorized are now u Time to Exploit Various Devic Motorola Focus 73 Outdoor WiFi Cam Asus AC66u Wireless Router TP LINK TL-1043ND Wireless Router D-UNK DIR-865L Hello Baby Monitor TCP Connected SmartLED Light Bull Belkin N300 Wireless Router Netgear ReadyNas Network Attached St Pogoplug Mobile Wireless Backup Dev Seagate Disk Station Network Attached Belkin N900 Wireless Router Control4 HC-250Home Theater Controls 50 75 100 125	to disable your humble beginnin ntrol motorized are now used by Time to Exploit Various Devices Motorola Focus 73 Outdoor WiFi Camera Asus AC66u Wireless Router TP LINK TIL-1043ND Wireless Router TP LINK TIL-1043ND Wireless Router D-LINK DIR-865L Hello Baby Monitor TCP Connected SmartLED Light Bulb Belkin N300 Wireless Router Netgear ReadyNas Network Attached Storage Pogoplug Mobile Wireless Backup Device Seagate Disk Station Network Attached Storage Western Digital Disk Station Network Attached Storage Belkin N900 Wireless Router Control4 HC-250Home Theater Control System 50 75 100 125 150	to disable your humble beginnings at en htrol motorized are now used by tech Time to Exploit Various Devices Motorola Focus 73 Outdoor WiFi Camera Asus AC66u Wireless Router TP LINK TL-1043ND Wireless Router TP LINK DIR-865L Hello Baby Monitor TCP Connected SmartLED Light Bulb Belkin N300 Wireless Router Netgear ReadyNas Network Attached Storage Pogoplug Mobile Wireless Backup Device Seagate Disk Station Network Attached Storage Western Digital Disk Station Network Attached Storage Belkin N900 Wireless Router Control4 HC-250Home Theater Control System 50 75 100 125 150 175	to disable your humble beginnings at emergin ntrol motorized are now used by tech giants Time to Exploit Various Devices Motorola Focus 73 Outdoor WiFi Camera Asus AC66u Wireless Router TP LINK TL-1043ND Wireless Router TP LINK TL-1043ND Wireless Router TCP Connected SmartLED Light Bulb Belkin N300 Wireless Router Netgear ReadyNas Network Attached Storage Pogoplug Mobile Wireless Backup Device Seagate Disk Station Network Attached Storage Western Digital Disk Station Network Attached Storage Belkin N900 Wireless Router Control4 HC-250Home Theater Control System 50 75 100 125 150 175 200			

Got Bugs?

Figure shows how many minutes it took for Wolf Den engineers to compromise various devices during the IoT Challenge at DEF CON 24 last month. How many are in your office? How many are in your home?

HAL 9000

This year at DEF CON 24. DARPA conducted its first ever Cyber Grand Challenge. This pitted seven

increasingly difficult for product vendors to stand out. Making a demonstrably secure product is difficult and expensive. The competing priorities of adding new features, getting to market quickly, and containing cost often result in unintentional security vulnerabilities. One possible solution - albeit a relatively low tech one - is the bake-off. Sunlight is the best disinfectant, and testing products against competitors out in the open under the watchful eye of public scrutiny is an important part of establishing confidence and benchmarking. As demonstrated by the list of popular products to the left, vulnerabilities are everywhere, and you cannot pretend to be immune to them. Those that take vulnerabilities head-on have the intellectual high ground to ask if similar flaws exist in competito

teams against each other in a fully autonomous Cyber Capture The Flag (CTF) event. A CTF typically consists of teams hosting services (think email or a website), while analyzing these services for security flaws. When exploits are created, teams use them to attack others while inoculating themselves. This year, teams demonstrated that computers could discover novel exploits, as well as weaponize them into attacks and defenses, without a human in the loop. Perhaps more concerning than the 2001: A Space Odyssey sound of robot-controlled Computer Network Defense/Operations is that only two traditional defense contractors participated in the challenge, with neither faring well. There is room for industry to help mitigate IoT security flaws, but the cost to play and a whimsical spirit.

rs' products.	requires exception	requires exceptional tech prowess					
	lan K. (571) 253-2522	(40					
com	lan@wolfdenassociates.com	Will@wo					

Will K. 04) 939-7364 fdenassociates.com