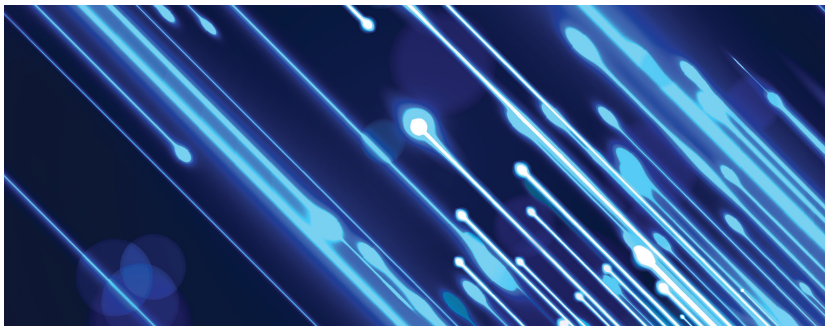
Hackers Exploit Critical Shellshock Vulnerability



Hackers are exploiting the recently discovered Shellshock command-line shell flaw, which lets them run commands on millions of servers, Macs, routers, and Internet-connected devices.

Information security companies have reported detecting hackers using the long present but previously undiscovered vulnerability to, for example, install malware on machines, add computers to botnets, launch distributed denial-of-service attacks, and conduct vulnerability scans against targets such as the US Department of Defense.

Security and reliability vendor Incapsula said in a company blog that its firewall blocked 217,000 exploit attempts on 4,000 domains in just the first four days after news of Shellshock broke. Eventually, Incapsula said, there were 1,970 attacks per hour originating from almost every country.

Analysis of the source code indicated that the vulnerability was in versions 1.13 (released in 1992) through 4.3 of the GNU Bourne Again Shell (Bash). Bash is the command-line shell used in many Linux and Unix operating systems, as well as several Mac OS X versions, and some Windows and IBM products.

Numerous Internet-connected devices, webservers, and online services run on Linux distributions that use Bash.

Companies like Apple and Akamai, as well as various Linux distributors such as Red Hat, Fedora, CentOS, Ubuntu, and Debian, have issued fixes for the Shellshock flaw.

However, security experts note, many users don't bother patching their machines, so a lot of systems are likely to have the bug for a long time.

If a system has a vulnerable Bash version as its default shell, hackers could exploit it via malicious Web requests, telnet communications, or other programs that use Bash to execute scripts.

Hackers could send a vulnerable system a request that includes data stored in an environmental variable, which contains information such as the directories in which files should be installed, where temporary files should be kept, and where user-profile settings can be found.

The hackers could malform the data so that Bash treats it as a command, allowing the attackers to run programs on and ultimately control the target system.

After 75 years, Hewlett-Packard Splits into Two Companies

Hewlett-Packard, one of Silicon Valley's oldest and most venerable tech firms, has decided to address its financial challenges by dividing itself into two companies.

The new companies will be Hewlett-Packard Enterprise, which will provide software, hardware, and services to corporate customers; and HP Inc., which will run the original firm's PC and printer businesses.

HP officials say they expect to complete the separation process by the end of next year.

The company approved the split as it begins the fourth year of the five-year turnaround plan initiated when chair, president, and CEO Meg Whitman began running HP.

As part of the plan, HP—which was struggling financially—initiated layoffs that are expected to total 55,000 by the time the split is finalized. The company had 317,500 employees a year ago.

Whitman said, "The decision to separate into two market-leading companies underscores our commitment to the turnaround plan. It will provide each new company with the independence, focus, financial resources, and flexibility they need to adapt quickly to market and customer dynamics."

Some industry observers applauded the move as making HP's operations more nimble and efficient at a time when the company appears to be recovering financially.

Others, though, say dividing HP won't change the firm's fortunes without a change in attitude that emphasizes technology innovation, as well as research and development.

After the split, Whitman will be chair of HP Inc. and CEO of Hewlett-Packard Enterprise. Patricia Russo, who currently serves on HP's board of directors, will be the chair of Hewlett-Packard Enterprise. Dion Weisler, currently HP's executive vice president for printing and personal systems, will become president and CEO of HP Inc.

Many people credit HP with helping to create Silicon Valley. After graduating with degrees in electrical engineering from Stanford University, Bill Hewlett and Dave Packard founded HP in 1935 in a rented Palo Alto, California, garage with an initial capital investment of $538.

Published by the IEEE Computer Society

Support Grows for New Software Approach That Could Advance Cloud Computing

Major technology companies such as Amazon and Google are backing a new open source approach that could boost cloud computing by making it easier to run applications on many types of systems across the Internet.

The firms are supporting Docker technology, a platform from Docker Inc. that developers can utilize to place applications in software containers. This would benefit cloud computing, because users could download the apps from the Internet or any private network and then run them on any Linux machine or cloud platform.

Proponents add that Docker will make developers' lives easier by letting them focus on designing programs without worrying about enabling the software to work on various machines or platforms.

Software containers aren't new, but supporters say Docker makes packaging applications and moving them among various types of machines easier.

According to Docker Inc., about 14,000 applications are now using its containers. eBay is employing the system to test new software in its datacenters. Google, which is trying to challenge Amazon's dominance in the cloud computing market, is also working with Docker.

The technology isn't without concerns.

For example, machines must download software enabling use of the containers. The software is supposed to run the same way on all Linux versions, but this isn't always the case. Some containers thus might not run on all versions. Docker Inc. says it's addressing this issue.

In addition, some cloud service providers are developing their own proprietary application-portability technologies and thus might not adopt or might even oppose Docker.

Users touch the Nymi wristband to activate it. The band then generates electrocardiogram readings, which it uses to authenticate wearers to computers, applications, and other systems.

New Technology Makes Authentication Just a Heartbeat Away

A Canadian startup has developed a smart wristband that uses wearers' unique electrocardiograms (EKGs) to authenticate them to applications, computers, payment devices, and other systems.

Bionym, based in Toronto, notes that its $99 Nymi band would eliminate the need to set, remember, and regularly change passwords. The company also claims its system is safer, as well as easier and less inexpensive to operate, than password-based schemes.

Venture capitalists Ignition Partners, Relay Ventures, MasterCard, and Salesforce Venture recently invested $14 million to commercialize the project.

To activate the system, users touch the Nymi to complete a circuit, which generates an EKG reading. The reading is uploaded via Bluetooth to a computer and processed by algorithms, which yield a digital key that is sent to a tamper-resistant part of the Nymi band.

This key represents a unique identity that users can transmit wirelessly via Bluetooth Low Energy technology to devices for automatic authentication and access.

The Nymi includes a proximity sensor that determines when the band is near enough to automatically log onto or far enough away to automatically log off of a device or application. The activation distance changes depending on the type of application involved. For example, the Nymi won't log onto a store's payment system unless it's very close to the point-of-sale device, to avoid inadvertent money transfers.

An accelerometer and gyroscope in the band give the system motion-detection capabilities, which let wearers create their own set of gestures to execute various functions.

Bionym has released a software developer's kit for building applications that work with the Nymi.

$10 Potato Salad Crowdfunding Gag Unexpectedly Benefits Charity

What started as a joke by Zack Brown of Columbus, Ohio, to raise $10 via Kickstarter for making a batch of potato salad yielded $55,492, which Brown recently used to help nonprofits fight hunger and homelessness in Central Ohio.

He started his Kickstarter page (www.kickstarter.com/projects/324283889/potato-salad) as a gag in July, not expecting a lot of traffic. However, as word of the unusual effort spread, Brown's page received 4.1 million views, making it the fourth-most-viewed project page in Kickstarter's history.

And by 2 August, 6,911 people from 74 countries had contributed money—and recipes.

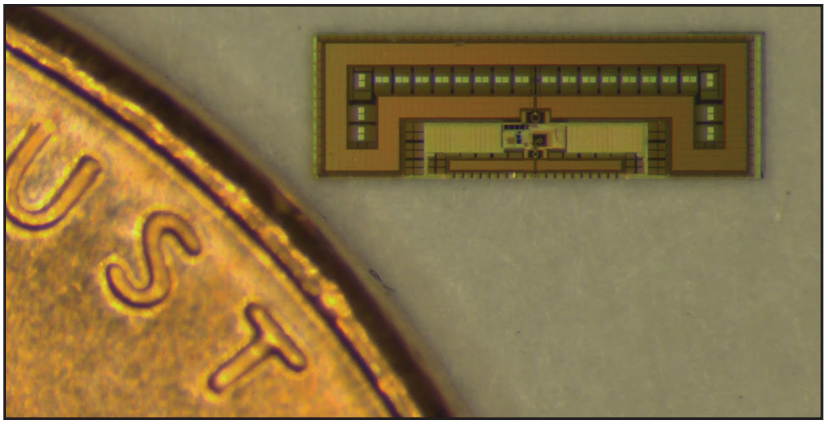
Brown used the revenue to produce the potato salad he promised to make and ship the incentive gifts—such as hats and T-shirts—he promised to large donors.

With the leftover cash, Brown decided to hold a party in a municipal park in his hometown to benefit charity.

Kickstarter prohibits people who run projects from giving their money directly to charities.

To get around this, Brown used his cash to pay for PotatoStock 2014 (http://thepotatostock.com), a free concert with concession stands, sponsorships, and, of course, potato salad.

He will use the revenue from the event to create a permanent fund to help nonprofit organizations in his native Central Ohio combat hunger and homelessness.



Researchers have developed a tiny, powerful, energy-efficient, inexpensive radio—shown here next to a US penny—that could fit in everyday devices and allow them to become part of the Internet of Things.

Exotic Web Tracking Tools Threaten Privacy

Three increasingly popular tools that help website owners track visitors so that they can target them with advertising threaten the privacy of Internet users, according to Catholic University Lueven and Princeton University researchers.

Sites have long utilized cookies to collect information about visitors—such as the webpages they view—to determine their interests and indicate which advertisements would be effective to show them. However, users can easily block or delete cookies.

To enable more persistent tracking, numerous websites now employ techniques such as canvas fingerprinting, evercookies, and cookie synching.

Canvas fingerprinting uses a browser's canvas API—which provides ways to create images—to, in essence, render a "fingerprint" of a person's online activities.

Evercookies are a JavaScript-based cookie that resists deletion by replicating itself in various places on a computer and re-creating itself if it finds that the user has deleted any copies.

When an advertiser buys cookie information from one domain, it can't automatically get its server, which is on another domain, to read the information and serve ads based on the data. Typically, a server can work only with cookies set to its own domain. *Cookie synching* addresses this by letting advertisers map user IDs from one system to another.

The Catholic University Lueven and Princeton researchers say the three approaches threaten privacy because users aren't aware they're being targeted by the technologies, don't know what data is being collected, and might not know how to avoid being tracked.

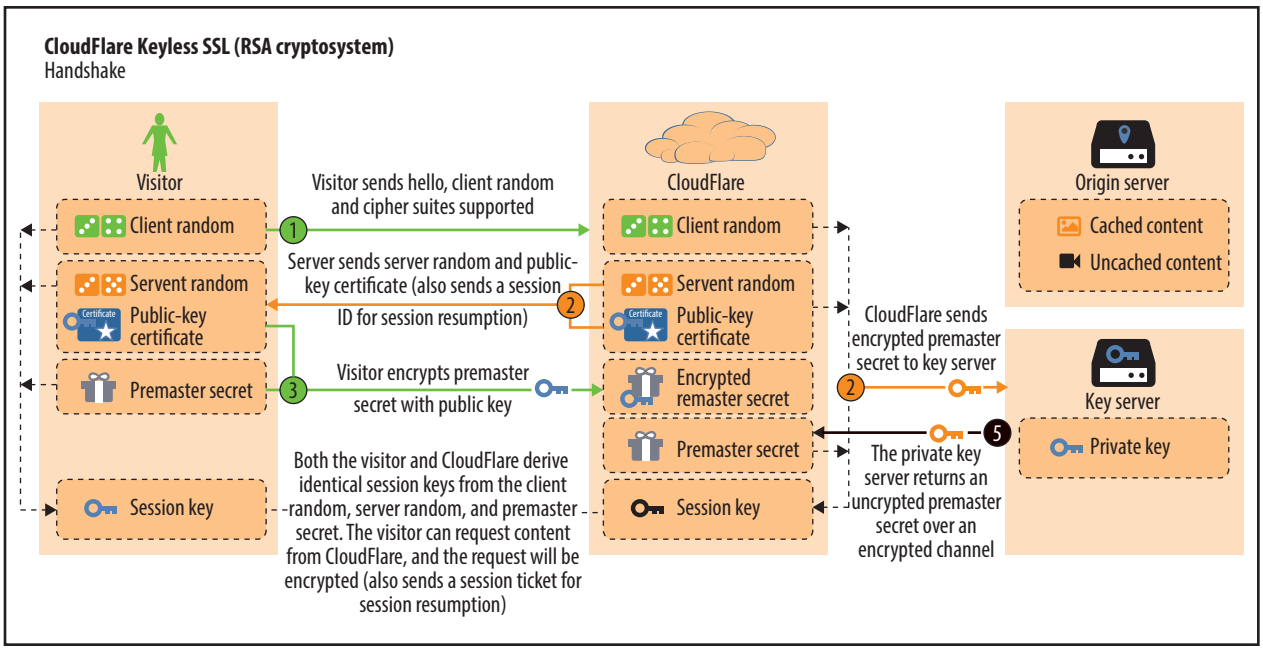
The scientists say they want their findings to enable users who don't want to be tracked to defend themselves and they want website owners held accountable for the technologies they deploy.

Scientists Build Tiny Radio That Could Advance the Internet of Things

Researchers have designed a tiny radio that could help hasten adoption of the Internet of Things (IoT).

In the IoT, everyday devices—like thermostats, home security systems, or refrigerators—connect online and either interact with one another autonomously or communicate with users.

The tiny new radio—which scientists from Stanford University and the University of California, Berkeley, developed—sits on a small chip that measures just a few millimeters on each side. It thus could fit within many types of IoT devices.



Vendor CloudFlare has developed Keyless SSL, which provides a way to securely store information in the cloud without also having to put private cryptographic keys there in a public-facing server. Source: CloudFlare

The radios offer considerable processing power and can compute, transmit, and execute the commands that devices send back and forth as part of the IoT.

The radios are very inexpensive—costing perhaps a few cents each to make in large quantities—in part because of their size.

This is critical because if the IoT is to become popular, many everyday devices will need to acquire controllers and communications capabilities economically, noted Stanford assistant professor Amin Arbabian.

The new radios are long lasting and energy efficient. And they don't need batteries because they gather power from the incoming electromagnetic signals.

New Networking Technology Could Make Security Products Ineffective

A new networking technology billed as a high-powered version of TCP could render firewalls and other security products useless in many circumstances, according to researchers.

Multipath TCP (MPTCP) is still being considered for standardization by the Internet Engineering Task Force. However, it's already used by Apple in its Siri voice-recognition software, and by both Cisco Systems and Juniper Networks in some of their equipment.

There are MPTCP implementations for operating systems such as Android, BSD, and Linux, but not yet for Windows.

Standard TCP uses just one connection path to send datasets. MPTCP, on the other hand, simultaneously utilizes multiple paths, which improves performance, resource usage, and robustness.

However, the new technology causes problems for security approaches such as firewalls and deep packet–inspection software, which were designed for standard TCP, noted researchers from security-service provider Neohapsis.

For example, to enable the use of multiple paths, MPTCP separates TCP data from a specific IP address. This means the packets in one dataset could come from multiple addresses. Thus, security products that process datasets coming from only one address at a time won't see all the incoming traffic and might miss malicious behavior.

In addition, the products might not be able to determine that multiple incoming MPTCP streams are part of the same dataset and thus might not link them together for analysis, the Neohapsis researchers said.

Network operators could try to cope with this by blocking all MPTCP packets, they added, but this won't be practical if and when the new technology becomes popular.

Service Offers New Approach to Cloud Security

A security vendor has released a new open source program designed to let users securely store data for future access in the cloud without also having to place their private cryptographic keys there.

CloudFlare's Keyless SSL lets users store the private keys on an internal, rather than a public-facing, server.

Workers with the US Federal Emergency Management Agency test the FINDER (finding individuals for disaster and emergency response) system that NASA's Jet Propulsion Laboratory developed to locate people buried in rubble after earthquakes or other destructive events.

The ability to better protect keys could overcome concerns that businesses handling sensitive data—such as financial and healthcare companies—have about keeping data in the cloud.

Typically, firms using the cloud store private keys on the same public-facing server that handles Web traffic. However, this could let hackers access the keys and compromise the security of data stored online.

In some cases, businesses use third parties to handle their Secure Sockets Layer systems. However, this places the keys out of the business' control.

With CloudFlare's new system, private SSL keys are maintained on customers' internal servers, which can sit behind firewalls or be secured in other ways.

To protect the communications involved in the process, the system transmits and processes key-signing requests via an encrypted tunnel to the user's server.

CloudFlare says it got the idea for the new product after being approached by financial institutions that had suffered cyberattacks.

The company plans to bundle Keyless SSL with its enterprise security service.

NASA System Will Find Disaster Survivors

NASA has developed software and radar-based remote-sensing technology that can find survivors buried in rubble after disasters.

Researchers at the space agency's Jet Propulsion Laboratory (JPL) are using the software in the FINDER (finding individuals for disaster and emergency response) system, which picks up subtle movements—even those generated by heartbeats and breaths—through 30 feet of debris or 20 feet of concrete, or over 100 feet of open space.

To detect motion, FINDER uses a low-power microwave radio signal that can repeatedly bounce off buried bodies and reflect back to the systems' radar, detecting movement in the process.

Software run on a laptop then identifies which movements represent heartbeats or other signs of life and filters out motions such as tree branches swaying, pieces of paper blowing about, or animals crawling.

JPL says the system could work in the aftermath of disasters such as earthquakes, tornadoes, hurricanes, and avalanches.

According to JPL, FINDER is easy to work with and requires perhaps 10 minutes to learn and set up. The US Federal Emergency Management Agency has tested it, but officials haven't had the opportunity to use the system in a disaster yet.

After the 2010 earthquake in Haiti—which killed an estimated 316,000 people and buried thousands more in collapsed buildings—the US Department of Homeland Security asked NASA engineering manager James Lux for help. Lux had designed a FINDER-like device for the US military that can determine whether a downed solider is still alive.

NASA develops technology but doesn't mass produce it. Federal officials will thus have to find a company to license FINDER and manufacture it in large quantities. JPL estimates each system will cost about $10,000 and could be available commercially within the next two years.

Meanwhile, Lux is looking for ways to reduce the device's size and mount it on a drone or helicopter. He is also working on similar technology that could enable firefighters to locate people in burning structures.

Editor: Lee Garber, *Computer*; l.garber@computer.org