Security Now! #585 - 11-08-16

The Windows AtomBomb

This week on Security Now!

- The answer to last week's security & privacy puzzler,
- Squarespace decides to encrypt,
- The open source LessPass app,
- LastPass goes mobile-free,
- Lots of problems with OAuth,
- New Internet services' privacy concerns,
- News from the IP spoofing front,
- Microsoft clarifies Win10 update settings and winds down EMET,
- A hacker finds a serious flaw in Gmail,
- MySQL patches need to be installed now,
- A tweet from Paul Thurrott,
- A bit of errata and... and the Windows Atombomb attack.

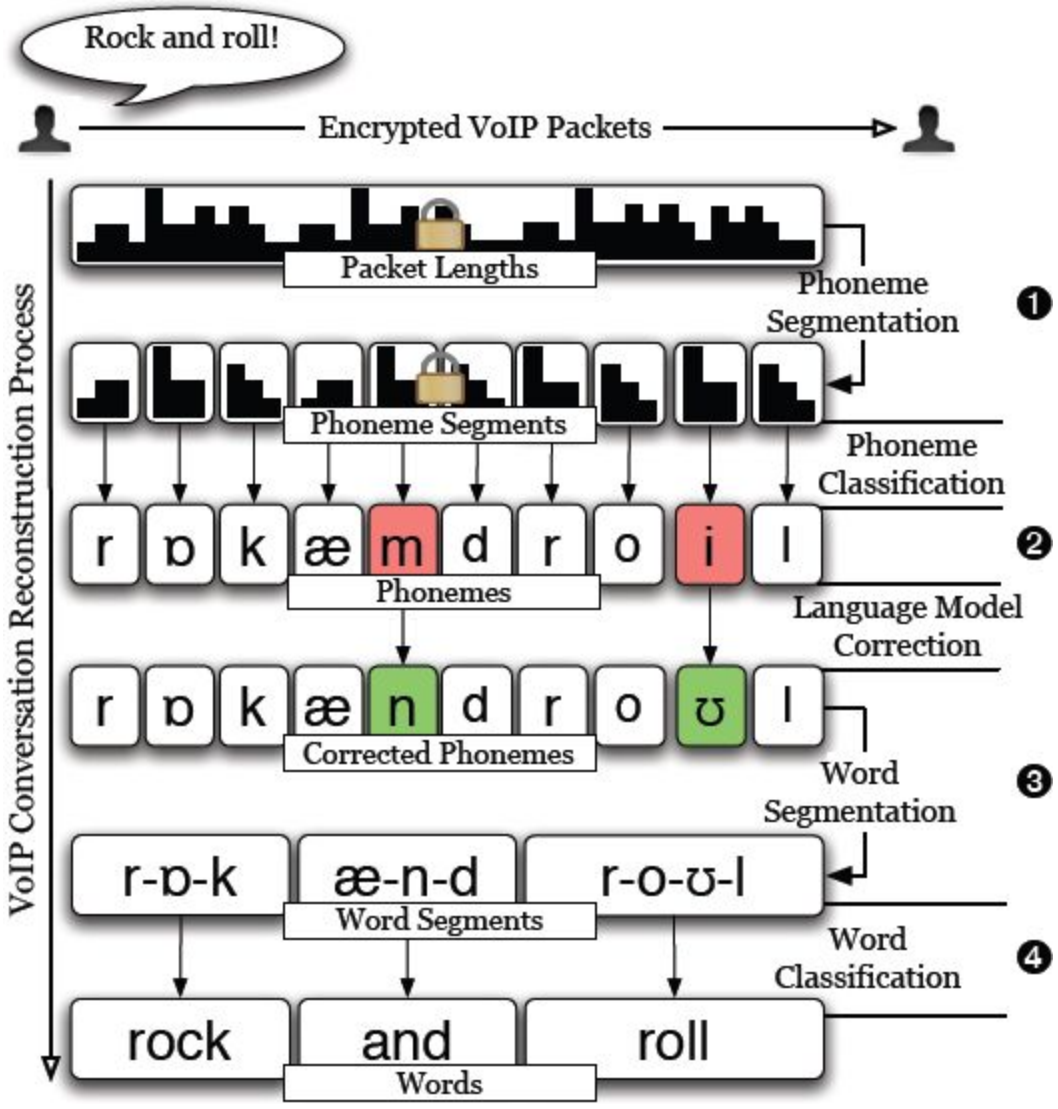
Last Week's Security/Privacy Puzzler

Common security practice dictates that compressible data should be compressed before it is encrypted because once any data has been encrypted it will become non-compressible. But… does compressing then encrypting create any threat to security or privacy?

YES!

The threat is to encryption's privacy guarantee: In any setting where sizing information of the original data survives encryption, a potential for information leakage exists. As we know, the efficiency of compression is determined by the information redundancy contained with the uncompressed data. We have already seen attacks on compressed and encrypted HTTPS sessions with the CRIME and BEAST attacks.

Researchers at the University of North Carolina at Chapel Hill have recently extended this by successfully attacking the encrypted voice-over-IP (VoIP) communications used by Skype, Fring, Google Talk, etc… **using the continuously varying size of the communications packets:**



Security News

Patch Tuesday

- November 2016, Security Monthly Quality Rollup for WIndows 7 for x64-based systems.
- For Win7: 134MB

Squarespace adopts Let's Encrypt SSL

- https://blog.squarespace.com/blog/were-securing-millions-of-websites-with-ssl
- As our regular listeners will know, SquareSpace is a TWiT Sponsor
- October 24th (2 weeks ago yesterday)
- <quote> Secure Sockets Layer, or SSL, is a technology that secures the connection between your browser and the website you're visiting. It allows you and your website visitors to feel confident that their information is secure. And we believe that confidence is an important part of your online identity.

  So, starting today, we're proud to offer free SSL on all Squarespace websites. Website owners should not have to pay extra or wrestle with complex technical issues to offer this basic security to their users. Every website can enable SSL, which will automatically direct users and search engines to a secure version of that site. The result is that millions of more domains on the Internet will be secured via SSL, our customers can take advantage of the confidence that secure websites bring users, and we will have helped the Internet take a huge step forward in promoting security by default. As an added benefit, websites hosted on Squarespace may enjoy a boost in search rankings.

  Squarespace is taking care of almost everything, making this an easy transition for customers. To seamlessly manage SSL certificates for all of our websites, we've partnered with Let's Encrypt, a free and open certificate authority (CA) run for the public's benefit that provides free SSL certificates. Current Squarespace users can see instructions on how to enable SSL on their site by checking out our Help guide.

"LessPass"

- https://lesspass.com/#/
- https://blog.lesspass.com/lesspass-how-it-works-dde742dd18a4#.10mdslmll
- Hope he doesn't attempt to obtain a trademark on that.
- (And he may still receive a cease and desist letter from LastPass's intellectual property attorneys.)
- Input:
  - Site's domain
  - Login name (eMail address)
  - Master Password
  - Specify:
  - abc / ABC / 123 / %!@ / Length / Integer Increment Modifier
- (Why SQRL doesn't offer this option.)

Get LastPass Everywhere: Multi-Device Access Is Now Free! | The LastPass Blog

- https://blog.lastpass.com/2016/11/get-lastpass-everywhere-multi-device-access-is-now-free.html/
- Last Wednesday, Joe Siegrist posted: I'm thrilled to announce that, starting today, you can use LastPass on any device, anywhere, for free. No matter where you need your passwords – on your desktop, laptop, tablet, or phone – you can rely on LastPass to sync them for you, for free. Anything you save to LastPass on one device is instantly available to you on any other device you use.

  I've seen postings from people ho have read only the headline and worried about how LastPass would then be making money.

  What changed is that the mobile platforms no longer require a premium account.

  LastPass continues to offer their free, premium ($1/month), and enterprise plans.

  <quote>
- Q: Why does LastPass require a Premium charge for the mobile apps?
  A: We give away the majority of our features and service for free, because we sincerely want to make password management accessible for everyone. We've determined that mobile access and a few other advanced features create "added value" for our customers, and the Premium service provides unlimited access to all of those added features.

  While we've striven to offer as much as we can for free, our Freemium business model allows us to maintain our service and further its development. We continue to add new features to both the free and Premium services that increase value for our users.

A comprehensive formal security analysis of OAuth 2.0
https://blog.acolyer.org/2016/11/07/a-comprehensive-formal-security-analysis-of-oauth-2-0/
https://infsec.uni-trier.de/people/publications/paper/FettKuestersSchmitz-CCS-2016.pdf

- A team of German university researchers conducted the first formal security analysis of Oauth 2.0

- Reminder: Oauth is the increasingly ubiquitous "Sign in with Facebook", "Sign in Twitter", etc.

- Why Steve is not a fan:
  - The protocol is exceedingly complex, has always felt like an inherently error prone kludge.
  - Bouncing your web browser around among sites just feels wrong.
  - It's a 3-party solution which leaks privacy information to the Identity Provider (The identity provider knows who you are and everywhere you login on the web... so you bet they are happy to offer the service.)

- A 95-page technical report!
- <quote> The OAuth 2.0 protocol is one of the most widely deployed authorization/single

sign-on (SSO) protocols and also serves as the foundation for the new SSO standard OpenID Connect. Despite the popularity of OAuth, so far analysis efforts were mostly targeted at finding bugs in specific implementations and were based on formal models which abstract from many web features or did not provide a formal treatment at all.

In this paper, we carry out the first extensive formal analysis of the OAuth 2.0 standard in an expressive web model. Our analysis aims at establishing strong authorization, authentication, and session integrity guarantees, for which we provide formal definitions.

Our modeling and analysis of the OAuth 2.0 standard assumes that security recommendations and best practices are followed in order to avoid obvious and known attacks.

When proving the security of OAuth in our model, we discovered four attacks which break the security of OAuth. The vulnerabilities can be exploited in practice and are present also in OpenID Connect.

We propose fixes for the identified vulnerabilities, and then, for the first time, actually prove the security of OAuth in an expressive web model. In particular, we show that the fixed version of OAuth (with security recommendations and best practices in place) provides the authorization, authentication, and session integrity properties we specify.

The problems were reported to the OAuth and OpenID Connect working groups who confirmed the attacks.

Over 1 Billion Mobile App Accounts can be Hijacked Remotely with this Simple Hack

- http://thehackernews.com/2016/11/android-oauth-hacking.html
- Forbes: This Hack Can Silently Break Into 1 Billion Android App Accounts
    - http://www.forbes.com/sites/thomasbrewster/2016/11/03/this-hack-can-break-into-1-billion-android-app-accounts/
- Meanwhile, a trio of Chinese researchers from the Chinese University of Hong Kong (located right next to the post office) presented their unrelated Oauth findings last week at BlackHat Europe 2016.

- The researchers carefully examined 600 of the most popular US and Chinese Android apps. In 41% of the 182 apps which supported OAuth single sign-on they found problems associated with OAuth 2.0.

- Many iOS and Android apps offering Oauth have failed to rigorously follow the standard.

- When testing real world implementations, the researchers found that the developers of a huge number of Android apps were not properly checking the validity of the information sent from the ID provider, like Facebook, Google or Sina.

- The vulnerabilities resided in the way many app developers implemented OAuth. When a user logs in via OAuth, the app should check with the ID provider, like Facebook, Google or Chinese firm Sina, that they have the correct authentication for those sites. If so,

OAuth provides an access token from the ID provider's server which is issued to the server of the mobile app. This allows the app server to gather the user's authentication information and let them login with their Facebook or Google credentials.

But the researchers found that for many Android apps (and iOS is every bit as troublesome), the app developers did not bother to properly verify the validity of the information returned by the ID provider. They failed to verify the signature attached to the authentication information retrieved from Facebook and Google. In other cases, the app server would only look at the returned user ID and log the individual in without checking the attached OAuth information to see if they were linked.

As a consequence, it's possible for a remote hacker to download the vulnerable app, login with their own information, then change the username to that of the target individual by using a server set up to tamper with the data sent from Facebook, Google or any other ID provider. Those usernames could either be guessed or retrieved with some simple Googling. Because these OAuth-using apps never bother to actually verify the signature provided by the ID provider, the name change goes undetected.... granting the attacker total control of the data held within the app.

- The researchers suggest:
    - Unclear developer document.
    - OAuth was originally designed for websites, not for apps.
    - Implementation errors by some identity providers.

UK car insurer Admiral to use Facebook data to decide how to rate customers

- FirstCarQuote: How do I get a quote? The firstcarquote online app is really easy to use:
    - Enter car registration
    - Agree our terms and conditions
    - Connect with Facebook
    - Answer 10 simple questions
    - Get quote
    - Call us to buy your cover
- *November 1st:*
- https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts
- "Admiral to price car insurance based on Facebook posts"
- Insurer's algorithm analyses social media usage to identify safe drivers in unprecedented use of customer data
- <quote> One of the biggest insurance companies in Britain is to use social media to analyse the personalities of car owners and set the price of their insurance. The unprecedented move highlights the start of a new era for how companies use online personal data and will start a debate about privacy. Admiral Insurance will analyse the Facebook accounts of first-time car owners to look for personality traits that are linked to safe driving. For example, individuals who are identified as conscientious and well-organised will score well. The insurer will examine posts and likes by the Facebook user, although not photos, looking for habits that research shows are linked to these traits. These include writing in short concrete sentences, using lists, and arranging to

meet friends at a set time and place, rather than just "tonight". In contrast, evidence that the Facebook user might be overconfident – such as the use of exclamation marks and the frequent use of "always" or "never" rather than "maybe" – will count against them.

- *November 2nd:*
- http://www.theverge.com/2016/11/2/13496316/facebook-blocks-car-insurer-from-using-user-data-to-set-insurance-rate
- "Facebook blocks insurer exploiting user data to find 'conscientious' drivers"
- Admiral Insurance wanted to analyze Facebook users' posts to see if they would make good drivers
- <quote> Facebook has blocked one of the UK's biggest insurers from using the social media network's user data to set insurance rates. A recently-launched scheme from Admiral Insurance targeted first-time car owners, offering to analyze their Facebook posts to see if their personality traits matched those of successful drivers. Participants were told they could save as much as £350 ($429) a year on their car insurance if they were judged to be conscientious and well-organized.

  The scheme, named firstcarquote, was set to launch this week, but, as first noted by UK privacy advocates Open Rights Group, the app has been blocked by Facebook from accessing user data. The initiative from Admiral Insurance would contravene Facebook's Platform Policy, which states that developers cannot "use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan."

Uber has serious privacy issues

- Uber's Privacy Woes Should Serve As a Cautionary Tale for All Companies
- https://www.wired.com/insights/2015/01/uber-privacy-woes-cautionary-tale/
- <Wired> Revelations from the Washington Post and others are bringing to light growing concern that every Uber employee, and apparently interviewee, is allowed unlimited access to customer data. For instance, one article described how the company's employees use a feature called "God View" that allows tracking of all Uber customers in real time; that information has then been displayed as entertainment at company parties. Another article cited an instance in which Uber senior executives examined the travel records of reporters who might write critically about the company, with Uber Senior Vice President Emil Michael going so far as speaking publicly of his desire to spend $1 million to dig up information on "your personal lives, your family." One article even cited how company officials analyzed ride data to predict overnight sexual liaisons, which the company called "Rides of Glory."

  If any of these allegations are true, then the company could be in violation of both federal and state privacy laws governing the handling of personal data and may be exposing themselves to serious risks and fines in the event this data is leaked or misused.

  Personally Identifiable Information (PII) is highly regulated across the globe by dozens of international privacy acts, from the US Privacy Act to the EU Privacy Directive. In fact, the US Privacy Act, which currently applies only to US Federal agencies, may be a good starting point.

NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

The data collected by Uber, including name, credit card information, current location and regularly travelled locations such as home and place of work, would likely fall into the second part of this definition.

No organization should give all employees unfettered access to such a vast treasure trove of customer or employee data unless it is pertinent to their role. The fact that Uber gave not just employees, but also interviewees, unlimited access to customer data is shocking, and their reported misuse of travel details for personal agendas has opened the company up to scrutiny by regulatory agencies around their privacy practices.

- Richard Stallman
    - https://stallman.org/uber.html
    - Reasons not to use Uber:
      We should not accept the promotional term "sharing economy" for companies like Uber. That is spin. A more accurate term is "piecework subcontractor economy". Because I reject technology that mistreats me, I will never order or pay for an Uber car. I hope there will always be taxis I can use. But what about you?

GCHQ wants internet providers to rewrite systems to block hackers

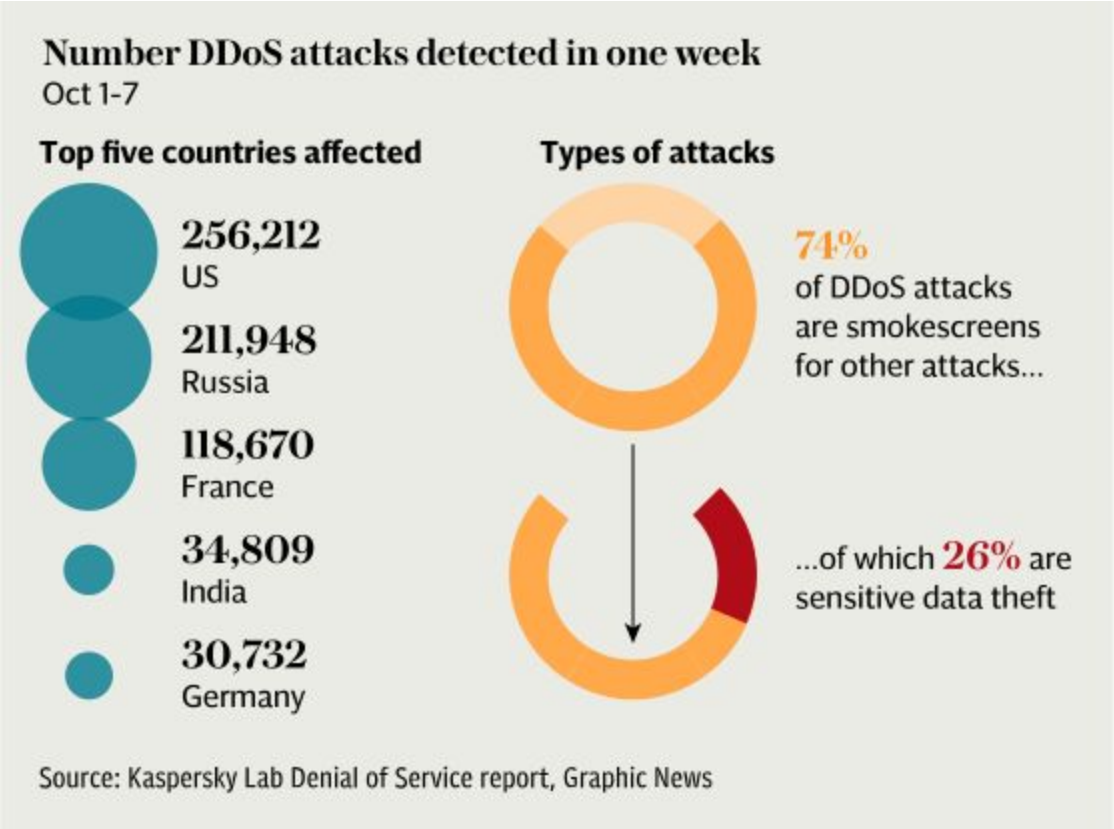
- http://www.telegraph.co.uk/technology/2016/11/05/gchq-wants-internet-providers-to-rewrite-systems-to-block-hacker/
- GCHQ is urging internet providers to change long-standing protocols to stop computers from being used to set off large-scale cyber attacks.

- The Government's cyber-defence arm said it plans to work with networks such as BT and Virgin Media to rewrite internet standards to restrict "spoofing" - a technique that allows hackers to impersonate other computers and manipulate them to carry out anonymous attacks.

- Ian Levy, technical director of GCHQ's National Cyber Security Centre, told the Sunday Telegraph: "We think we can get to a point where we can say a UK machine can't participate in a DDoS attack. We think that we can fix the underpinning infrastructure of the internet through implementation changes with ISPs and CSPs [communications service providers]."

- The plan would involve changes to the Border Gateway Protocol (BGP) and Signalling System 7 (SS7) standards that have been in place for decades, and are widely used for routing traffic. GCHQ wants providers to stop the trivial re-routing of UK traffic and help prevent text message scams.

The Internet Service Providers Association (ISPA), the body that represents ISPs, expressed scepticism, saying GCHQ was applying a "we can fix it , it's easy" approach to a complex, historic system.



CAIDA - Center for Applied Internet Data Analysis

- https://www.caida.org/projects/spoofer/
- A long time ago, they were tracking DDoS attacks by catching spoofed bounce packets.
- <quote> Seeking to minimize Internet's susceptibility to spoofed DDoS attacks, we are developing and supporting open-source software tools to assess and report on the deployment of Source Address Validation (SAV) best anti-spoofing practices. This project includes applied research, software development, new data analytics, systems integration, operations and maintenance, and an interactive analysis and reporting service.

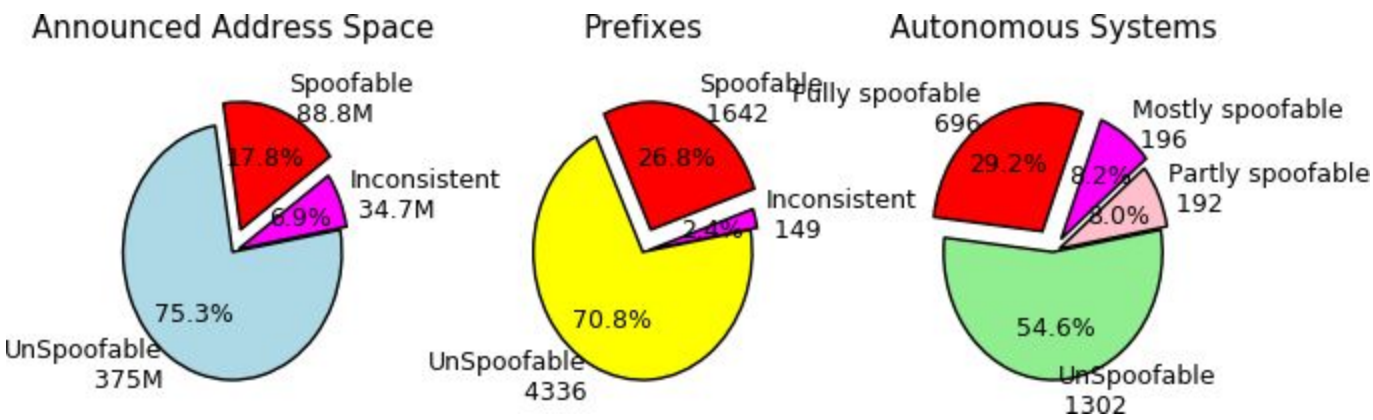
  We have developed and support a new client-server system for Windows, MacOS, and UNIX-like systems that periodically tests a network's ability to both send and receive packets with forged source IP addresses (spoofed packets). We are (in the process of) producing reports and visualizations that will inform operators, response teams, and policy analysts. The system measures different types of forged addresses, including private and neighboring addresses. The test results will allow us to analyze characteristics of networks deploying source address validation (e.g., network location, business type).

- Home > Projects > Spoofer
  - Windows, Mac OSX, Ubuntu, Source

- Results for my home IP a Cox:
  - IPv4:
  - ASN: 22773
  - Spoofed private addresses: Blocked.
  - Spoofed routable addresses: Blocked.

- Your host is behind a NAT router or firewall which rewrites the source addresses of the test traffic. To test your provider's network further, you must remove the NAT/firewall/router and connect directly.

- https://spoofer.caida.org/summary.php



Manage device restarts after updates (Windows 10)

- https://technet.microsoft.com/en-au/itpro/windows/manage/waas-restart
- Applies to Windows 10:
- <quote> You can use Group Policy settings or mobile device management (MDM) to configure when devices will restart after a Windows 10 update is installed. You can schedule update installation and set policies for restart, configure active hours for when restarts will not occur, or you can do both.

  <quote> After an update is installed, Windows 10 attempts automatic restart outside of active hours. If the restart does not succeed after 7 days (by default), the user will see a notification that restart is required. You can use the Specify deadline before auto-restart for update installation policy to change the delay from 7 days to a number of days between 2 and 14.

Microsoft to "End of Life" their Enhanced Mitigation Experience Toolkit (EMET)

- https://blogs.technet.microsoft.com/srd/2016/11/03/beyond-emet/
- Goodbye EMET: Microsoft sees no further need for the tool for modern software and OS that surpass it natively blogs.technet.microsoft.com/srd/2016/11/03?
- https://blogs.technet.microsoft.com/srd/2016/11/03/beyond-emet/
- <quote> Microsoft's Trustworthy Computing initiative was 7 years old in 2009 when we first released the Enhanced Mitigation Experience Toolkit (EMET). Despite substantial

improvements in Windows OS security during that same period, it was clear that the way we shipped Windows at the time (3-4 years between major releases) was simply too slow to respond quickly to emerging threats. Our commercial customers were particularly exposed since it often took years to deploy new OS versions in large scale environments. And thus, EMET was born as a stop-gap solution to deliver tactical mitigations against certain zero-day software vulnerabilities.

For Microsoft, EMET proved useful for a couple of reasons. First, it allowed us to interrupt and disrupt many of the common exploit kits employed by attackers at the time without waiting for the next Windows release, thus helping to protect our customers. Second, we were able to use EMET as a place to assess new features, which directly led to many security innovations in Windows 7, 8, 8.1, and 10.

But EMET has serious limits as well – precisely because it is not an integrated part of the operating system. First, many of EMET's features were not developed as robust security solutions. As such, while they blocked techniques that exploits used in the past, they were not designed to offer real durable protection against exploits over time. Not surprisingly, one can find well-publicized, often trivial bypasses, readily available online to circumvent EMET.

Second, to accomplish its tasks, EMET hooks into low-level areas of the operating system in ways they weren't originally designed. This has caused serious side-effects in both performance and reliability of the system and the applications running on it. And this presents an ongoing problem for customers since every OS or application update can trigger performance and reliability issues due to incompatibility with EMET.

Finally, while the OS has evolved beneath it, EMET hasn't kept pace. While EMET 5.5x was verified to run on Windows 10, its effectiveness against modern exploit kits has not been demonstrated, especially in comparison to the many security innovations built-in to Windows 10.

Hacker finds flaw in Gmail allowing anyone to hack any email account

- https://www.hackread.com/hacker-finds-gmail-hacking-flaw/
- Ahmed Mehtab, a student from Pakistan and the CEO of Security Fuse, discovered a flaw in Gmail's authentication or verification methods induced when a confirmation eMail bounces:

- If a user has more than one email address, Google lets the user link all of the addresses and also lets emails of the primary account be forwarded to secondary accounts.

- Mehtab identified an inherent flaw in the verification bypass method adopted by Google for switching and linking email addresses, which leads to the hijacking of the email IDs. He discovered that the email addresses became vulnerable to hijacking when one of the following conditions occurs:

    - When the SMTP of the recipient is offline
    - The email has been deactivated by the recipient

    - Recipient doesn’t exist or invalid email ID
    - The recipient does exist but has blocked the sender

- The attacker tries to verify the ownership status of an email address by emailing Google. Google sends an email to that address for verification. The email address cannot receive the email and hence, Google’s mail is sent back to the actual sender and this time it contains the verification code. This verification code is then used by the hacker and the ownership to that particular address will be confirmed.

Critical Flaws in MySQL Give Hackers Root Access to Server (Exploits Released)

- http://thehackernews.com/2016/11/mysql-zero-day-exploits.html
- In August, two severe 0-day vulnerabilities in MySQL and its MariaDB and PerconaDB forks were found and responsibly disclosed by Dawid Golunski of Legal Hackers.
    - MySQL Remote Root Code Execution (CVE-2016-6662)
    - Privilege Escalation (CVE-2016-6663)
- After more than 40 days have passed with both MariaDB and PerconaDB having released patches -- but Oracle not -- Dawid said he decided to go public with the details of the zero-days.
- Last Tuesday, he released proof-of-concept (POC) exploits for two vulnerabilities: One is the previously promised critical privilege escalation vulnerability (CVE-2016-6663), and another is a new root privilege escalation bug (CVE-2016-6664) that could allow an attacker to take full control over the database.
- Both the vulnerabilities affect MySQL version 5.5.51 and earlier, MySQL version 5.6.32 and earlier, and MySQL version 5.7.14 and earlier, as well as MySQL forks — Percona Server and MariaDB.
- MySQL has fixed the vulnerabilities and all of the patches ultimately found their way into Oracle's quarterly Critical Patch Update last month.
- If your systems are depending upon MySQL, make sure you've applied the latest patches.

Paul Thurrott (@thurrott)

- "Here we go again: Microsoft's popping up ads from the Windows 10 toolbar". So we get to be the customer AND the product!

Errata

- The serious trouble with bookmarking sites by IP...
- It totally breaks HTTPS and Multihosting

SpinRite

Norm in Thailand
Subject: Spinrite drive orientation

Hi Steve,
I have been searching for an updated answer for this but I would like to get confirmation on drive orientation when using SpinRite. I am sure this was covered before but I cannot find it. I have been using SpinRite for a very long time. Normally I have all drives mounted flat board down. My newer NAS has some problems with one new drive and I am planning to run SpinRite on all the drives. I have a new mini computer now for running SpinRite which is under test now and seems to be doing fine. The new NAS has the drives installed vertically on their side.
So the question is; should newer HDD's be done in maintenance mode(4) with the drive in the orientation that it will be installed in? I think on your new computer they are mounted vertical if I recall, did you run SpinRite in that same orientation?
Just for information does the drive run upside down make a difference on newer drives?
Thanks, Norm

The Windows AtomBomb

- http://blog.ensilo.com/atombombing-a-code-injection-that-bypasses-current-security-solutions
- https://breakingmalware.com/injection-techniques/atombombing-brand-new-code-injection-for-windows/
- ttp://thehackernews.com/2016/10/code-injection-attack.html
- http://www.darkreading.com/vulnerabilities---threats/atombombing-microsoft-windows-via-code-injection/d/d-id/1327320

EnSilo's Tal Liberman did a beautiful bit of creative engineering.

AtomBombing is performed only by using long-established features of every Windows operating system. There is no need to exploit an operating system bug or vulnerabilities... so there's nothing to patch, and Microsoft cannot, at this point, significantly change or remove these longstanding features.

However, anti-malware, including Microsoft's native A/V, will likely quickly adopt some augmented heuristics in an effort to defect the use of the technique Tal has developed.

About Global Atom Tables
https://msdn.microsoft.com/en-us/library/windows/desktop/ms649053(v=vs.85).aspx

Open Source Exploit demo code on Github:
https://github.com/BreakingMalwareResearch/atom-bombing
The trouble with Return Oriented Programming is that it is difficult to get a collection of tiny end-of-subroutine stubs to perform anything super useful. This is why ROP is typically used in

conjunction with buffer overruns, where the overrun creates the opportunity for an attacker to inject data -- which is later executed -- into the vulnerable victim process. Then the ROP is used to cause the victim to jump to and execute the injected data.

So, what Tal needed was to find a new way of injecting potential attack code into a victim process. The Windows core API "Global Atom Tables" makes this, at least in principle, possible.

What are "Global Atom Tables" ??

Armed with a concept, Tal then proceeded to weaponize the use of the Global Atom Table.

He worked out an ROP (return oriented programming) means for bootstrapping a tiny piece of ROP code, which involved just a few Windows APIs, to cross-load a buffer, kindly provided to the ROP code running in the victim, by a call to the Global Atom Table.

The moral of this story is: Apparently benign features can too often be abused by clever attackers.