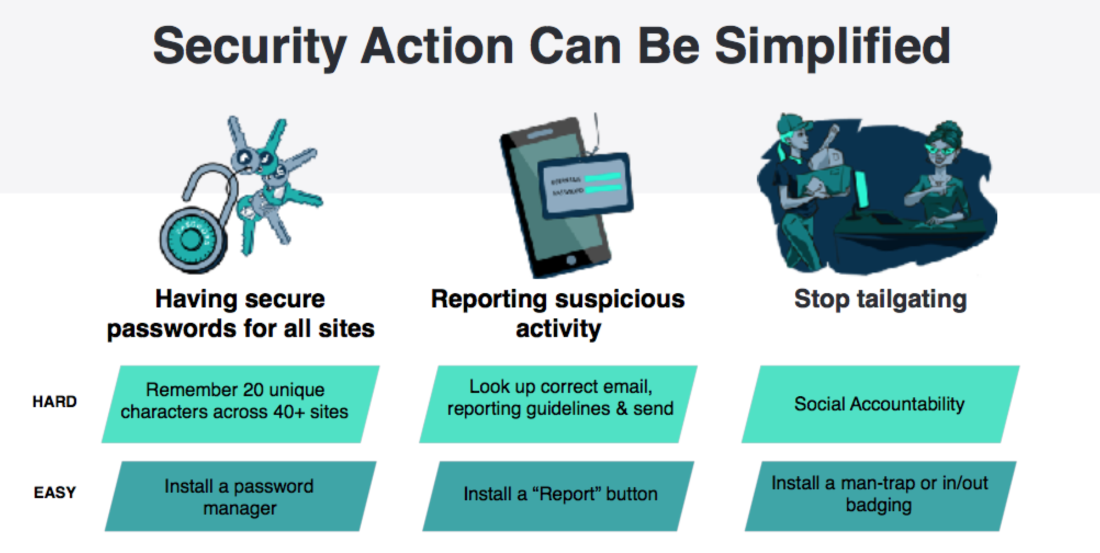
kindred

Security Newsletter

22 January 2018

Subscribe to this newsletter

Wanna motivate staff to be more secure? Don't bother bribing 'em



Security Action Can Be Simplified

	Having secure passwords for all sites	Reporting suspicious activity	Stop tailgating
HARD	Remember 20 unique characters across 40+ sites	Look up correct email, reporting guidelines & send	Social Accountability
EASY	Install a password manager	Install a "Report" button	Install a man-trap or in/out badging

It's frustrating getting users to keep information and systems secure on a daily basis. However, don't try any smart gimmicks – particularly offering wedges of cash or other prizes for good behavior. It doesn't work. Quite the opposite, it can make things worse.

Paying out a bonus to those who make few or zero security mistakes ultimately demotivates staff, Masha Sedova, cofounder of Elevate security, told Usenix's Enigma 2018 security conference. This is, in part, because once an incentive – especially a financial one – is dangled as a carrot, it's usually never substantial enough to warrant the extra effort required to follow security best practices. Thus, most people don't bother at all to meet the standard, reducing overall security.

Another, er, motivational technique – naming and shaming of employees by the BOFH – doesn't work either. Sedova said this massively demotivates staff. Instead, IT security teams need to be more positive with users. And by positive, she meant that workers should be praised for good behavior, and be given better tools to tackle threats to the network.

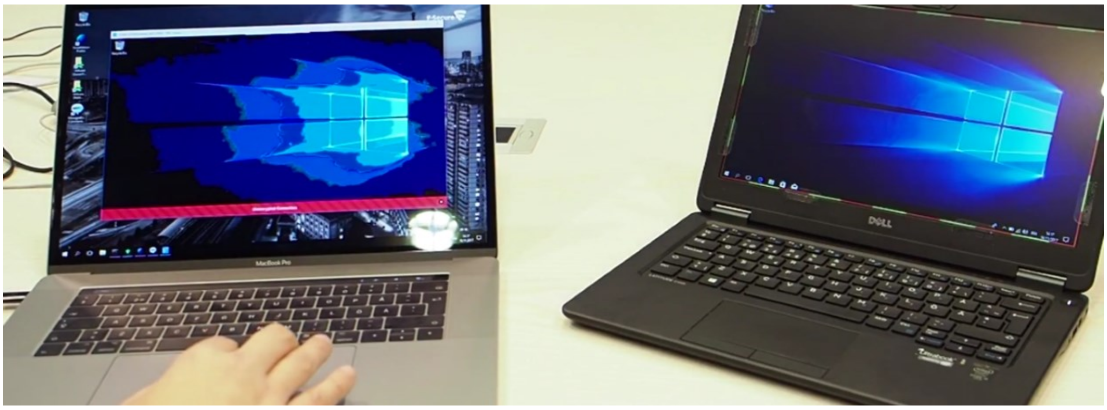
Sedova said that research, and her experience, shows that around 20 per cent of the workforce are very motivated to secure their systems. Around 70 per cent are ambivalent about it and will use security if it's easy enough, but 10 per cent won't touch security at all – and in the latter case, naming and shaming may be the only option.

research also revealed that Facebook users are more concerned about the security of their friends and family than they are about their own accounts. This means it should be possible to make security awareness spread in a viral way. "Reminding family about security techniques can be very effective in changing behavior," Das said. "But it has limitations – warn people too often and you're seen as a nag."

Read More

Presentation slides

Intel AMT Security Issue Lets Attackers Bypass BIOS and BitLocker Passwords



An F-Secure security researcher has found a way to use Intel's Active Management Technology (AMT) to bypass BIOS passwords, BitLocker credentials, and TPM pins and gain access to previously-secured corporate computers. Only laptops and computers on which Intel AMT has been provisioned (configured) are vulnerable, according to F-Secure security researcher Harry Sintonen, the one who claims to have discovered the issue last July.

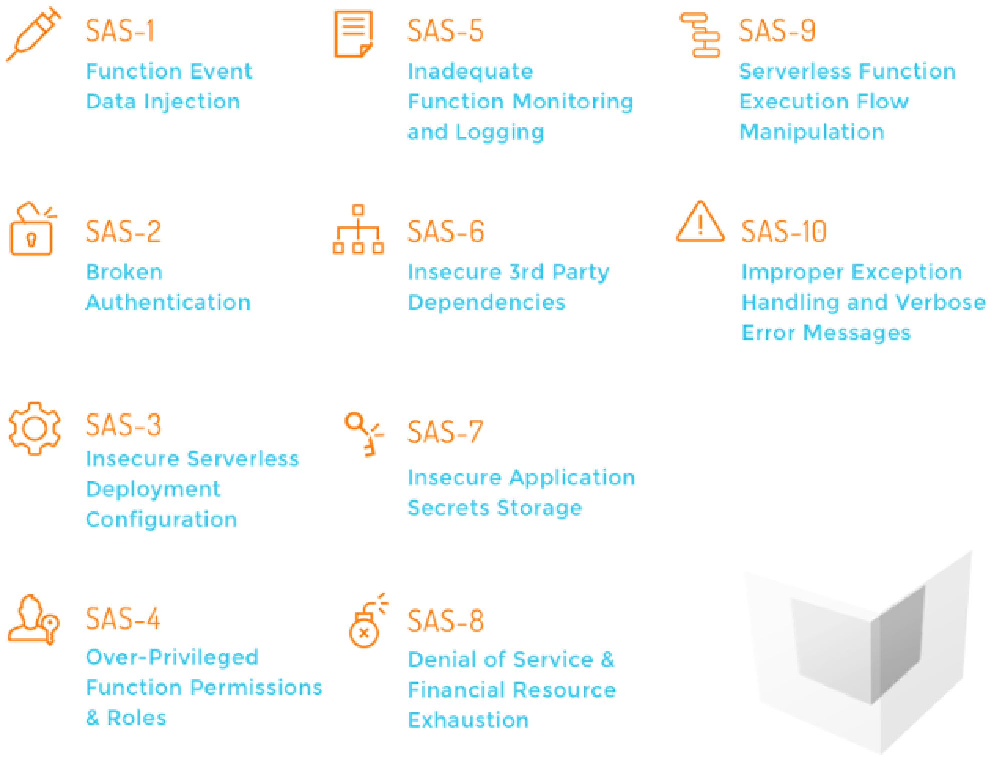
Computers on which AMT has been configured without an AMT password are vulnerable. He says a malicious actor with access to the device can press CTRL+P during the boot-up process and select the Intel Management Engine BIOS Extension (MEBx) for the boot-up routine, effectively bypassing any previous BIOS, BitLocker, or TPM logins. A MEBx password is required, but Sintonen says that in most cases companies do not change the default, which is "admin."

Most security experts scoff at the idea of attacks requiring "physical access" to perform and often demean their importance of such issues compared to other security bugs. But because this attack takes under a minute to perform and configure the device for future remote access. Sintonen recommends that companies configure an AMT password so attackers wouldn't be able to boot via MEBx and compromise the system. Optionally, unlike the Intel Management Engine (ME), AMT can be disabled, an option that Sintonen also recommends in situations where AMT use is not a corporate policy.

Read More

Original statement from F-Secure

The First "Serverless Architectures Security Top 10" Guide Released



SAS-1
Function Event Data Injection

SAS-2
Broken Authentication

SAS-3
Insecure Serverless Deployment Configuration

SAS-4
Over-Privileged Function Permissions & Roles

SAS-5
Inadequate Function Monitoring and Logging

SAS-6
Insecure 3rd Party Dependencies

SAS-7
Insecure Application Secrets Storage

SAS-8
Denial of Service & Financial Resource Exhaustion

SAS-9
Serverless Function Execution Flow Manipulation

SAS-10
Improper Exception Handling and Verbose Error Messages

PureSec is launching the “Serverless Architectures Security Top 10” project - this project is meant to provide assistance and education for organizations looking to adopt serverless architectures. This document is not a secure coding best practices, but rather a list of the top most common weaknesses that are found in serverless applications.

Serverless architectures enable organizations to build and deploy software and services without having to own or provision any physical or virtual servers. Applications built using serverless architectures are suitable for a wide range of services, and can scale elastically as cloud workloads grow.

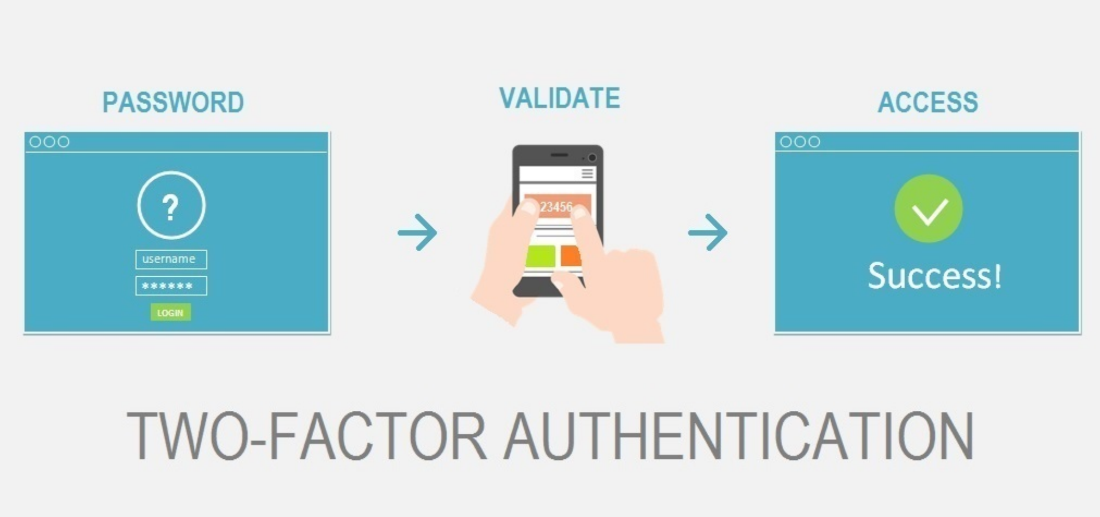
In essence, when you develop applications using serverless architectures, you relieve yourself from the daunting task of having to constantly apply security patches for the underlying operating system and application servers - these tasks are now the responsibility of the serverless architecture provider.

If you are a developer - this sounds like heaven, right? Hold on...there’s a fly in the ointment. You are still responsible for designing robust applications and making sure that your code doesn’t introduce application layer vulnerabilities. Moreover, any configuration related to the application itself or to cloud services it interacts with would still need to be secure - again, that’s your responsibility. In the serverless world, the cloud vendor and you share security responsibilities.

Read More

Whitepaper

Who's using 2FA? Sweet FA. Less than 1 in 10 Gmail users enable two-factor authentication



In a presentation at Usenix's Enigma 2018 security conference in California, Google software engineer Grzegorz Milka today revealed that, right now, less than 10 per cent of active Google accounts use two-step authentication to lock down their services. He also said only about 12 per cent of Americans have a password manager to protect their accounts, according to a 2016 Pew study.

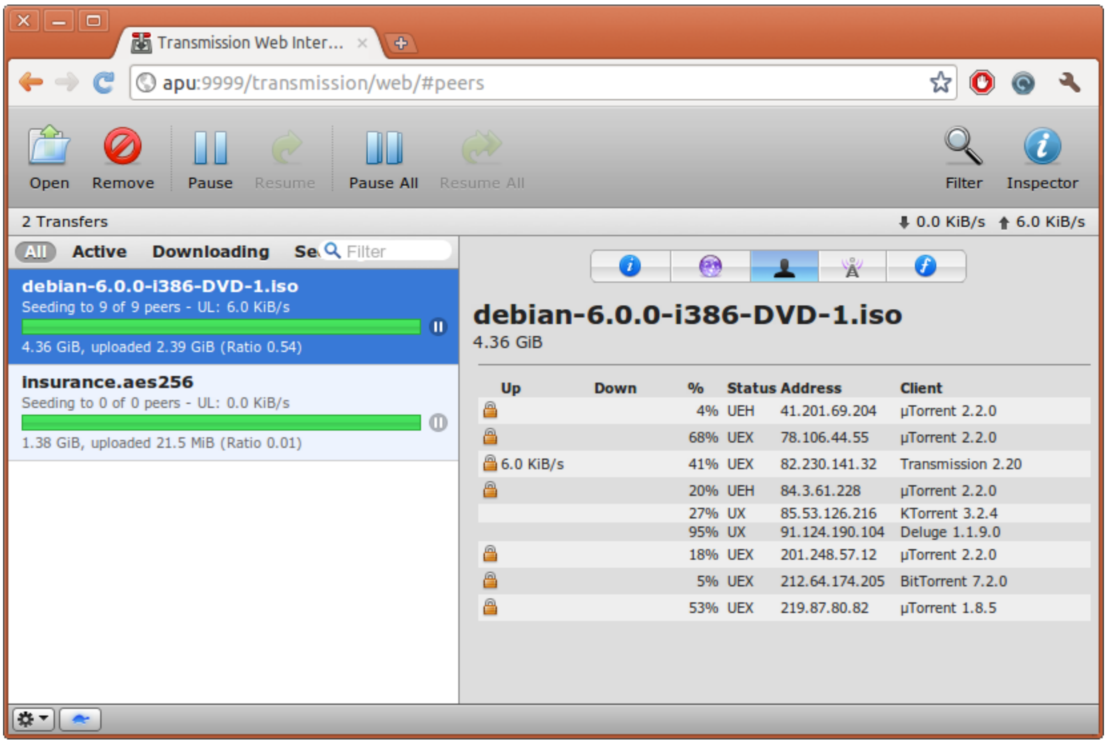
The Register asked Milka why Google didn't just make two-factor mandatory across all accounts, and the response was telling. “The answer is usability,” he replied. “It's about how many people would we drive out if we force them to use additional security.” Google has tried to make the whole process easier to use, but it seems netizens just can't handle it. More than 10 per cent of those trying to use the defense mechanism had problems just inputting an access code sent via SMS.

To spot criminals and other miscreants commandeering a victim's webmail inbox, the Chocolate Factory has increased its use of heuristics to detect dodgy behavior. A typical attacker has a typical routine – once they manage to get into an account, they shut down notification to the owner, ransack the inbox for immediately valuable stuff like Bitcoin wallet stuff or intimate photos, copy the contacts lists, and then install a filter to mask their action from the owner.

Please, if you haven't already done so, just enable two-step authentication. This means when you or someone else tries to log into your account, they need not only your password but authorization from another device, such as your phone. So, simply stealing your password isn't enough – they need your unlocked phone, or similar, to to get in.

Read More

Flaw in Popular Transmission BitTorrent Client Lets Hackers Control Your PC Remotely



2 Transfers ⬇ 0.0 KiB/s ⬆ 6.0 KiB/s

debian-6.0.0-i386-DVD-1.iso
Seeding to 9 of 9 peers - UL: 6.0 KiB/s
4.36 GiB, uploaded 2.39 GiB (Ratio 0.54)

insurance.aes256
Seeding to 0 of 0 peers - UL: 0.0 KiB/s
1.38 GiB, uploaded 21.5 MiB (Ratio 0.01)

debian-6.0.0-i386-DVD-1.iso
4.36 GiB

	Up	Down	%	Status	Address	Client
🔒			4%	UEH	41.201.69.204	µTorrent 2.2.0
🔒			68%	UEX	78.106.44.55	µTorrent 2.2.0
🔒	6.0 KiB/s		41%	UEX	82.230.141.32	Transmission 2.20
🔒			20%	UEH	84.3.61.228	µTorrent 2.2.0
			27%	UX	85.53.126.216	KTorrent 3.2.4
			95%	UX	91.124.190.104	Deluge 1.1.9.0
🔒			18%	UEX	201.248.57.12	µTorrent 2.2.0
🔒			5%	UEX	212.64.174.205	BitTorrent 7.2.0
🔒			53%	UEX	219.87.80.82	µTorrent 1.8.5

A critical vulnerability has been discovered in the widely used Transmission BitTorrent app that could allow hackers to remotely execute malicious code on BitTorrent users' computers and take control of them.

The PoC attack published by Ormandy exploits a specific Transmission function that lets users control the BitTorrent app with their web browser. Ormandy confirmed his exploit works on Chrome and Firefox on Windows and Linux (Fedora and Ubuntu) and believes that other browsers and platforms are also vulnerable to the attack. Ormandy found that a hacking technique called the "domain name system rebinding" attack could successfully exploit this implementation, allowing any malicious website that user visits to execute malicious code on user's computer remotely with the help of installed daemon service.

The loophole resides in the fact that services installed on localhost can be manipulated to interact with third-party websites. Attackers can exploit this loophole by simply creating a DNS name they're authorized to communicate with and then making it resolve to the vulnerable computer's localhost name.

Ormandy said the vulnerability (CVE-2018-5702) was the "first of a few remote code execution flaws in various popular torrent clients," though he did not name the other torrent apps due to the 90-day disclosure timeline.

Read More

Technical paper

Some Basic Rules for Securing Your IoT Stuff

Most readers here have likely heard or read various prognostications about the impending doom from the proliferation of poorly-secured "Internet of Things" or IoT devices. Loosely defined as any gadget or gizmo that connects to the Internet but which most consumers probably wouldn't begin to know how to secure, IoT encompasses everything from security cameras, routers and digital video recorders to printers, wearable devices and "smart" lightbulbs.

Throughout 2016 and 2017, attacks from massive botnets made up entirely of hacked IoT devices had many experts warning of a dire outlook for Internet security. But the future of IoT doesn't have to be so bleak. Here's a primer on minimizing the chances that your IoT things become a security liability for you or for the Internet at large.

Read More

Hacker Might Have Stolen the Healthcare Data for Half of Norway's Population

A hacker or hacker group might have stolen healthcare data for more than half of Norway's population, according to reports in local press. The attack took place on January 8 and came to light this week when Health South-East RHF, a healthcare organization that manages hospitals in Norway's southeast region, announced a security breach on its website.

Health South-East RHF manages healthcare units in nine of Norway's 18 counties. The list includes the counties of Akershus (includes Norway's capital Oslo), Aust-Agder, Buskerud, Hedmark, Oppland, Østfold, Telemark, Vest-Agder, and Vestfold. According to local press [1, 2], Health South-East RHF is the largest of Norway's four healthcare regions with hospitals serving 2.9 million of the country's total of 5.2 million inhabitants.

In the autumn of 2016, Health South-East RHF signed a contract with Hewlett Packard Enterprise to modernize its computer systems, but the contract was dropped after local press disclosed poor security controls when accessing patient healthcare information. The leak, if confirmed, is still nowhere near to what happened in Sweden, where a government contractor leaked the personal details of all the country's citizens. The person responsible was fined only a half a month's paycheck.

Read More

Cutting room floor

- LeakedSource Founder Arrested for Selling 3 Billion Stolen Credentials
- Common Approaches to Automated Application Security Testing - SAST and DAST
- Hackers Exploiting Three Microsoft Office Flaws to Spread Zyklon Malware
- OnePlus Site's Payment System Reportedly Hacked to Steal Credit Card Details
- AWS - How do we secure our datacenters
- Meltdown / Spectre patches compendium
- GhostTeam Android Malware Can Steal Facebook Credentials
- Google intros Security Center tool for G Suite
- Skygofree — Powerful Android Spyware Discovered
- Hawaii missile alert triggered by one wrong click
- Yes, Hawaii emergency management stuck a password on a sticky note
- MailChimp leaks your email address
- CloudFlair: Bypassing Cloudflare using Internet-wide scan data
- Aadhaar Getting Additional Security Layer
- Some thoughts on Spectre and Meltdown

#Tech and #Tools

- How to fix the Docker and UFW security flaw
- Bypassing CSP by Abusing JSONP Endpoints
- Leveraging Emond on macOS For Persistence
- pgen(1) – Passphrase Generator
- Exchange Web Services Cracker
- InSpectre: Test Spectre/Meltdown vulnerability

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us