CSNOG 2018


Report of Contributions

Contribution ID : **2** Type : **not specified**

BIND 9 Past, Present, and Future

Tuesday, 12 June 2018 14:00 (30)

BIND 9 is now 17 years old, the latest stable version 9.12.1 was released in March 2018 and the BIND 9 Team has adopted changes to adapt to the ever changing Internet landscape to be a truly open open-source software.

Type of Presentation

Primary author(s) : SURÝ, Ondřej (Internet Systems Consortium)

Track Classification : CSNOG1

Contribution ID : **9** Type : **not specified**

Zvyšujeme bezpečnost provozu .CZ DNS

Monday, 11 June 2018 17:30 (25)

Stav upgradu infrastruktury .CZ DNS anycastu a možnosti zapojení ISP do tohoto projektu.

Type of Presentation

Primary author(s) : BRŮNA, Zdeněk

Track Classification : CSNOG1

Contribution ID : **11** Type : **not specified**

WPAD a bezpecnost v DNS

Tuesday, 12 June 2018 11:25 (25)

Chteli bychom sitovou verejnost upozornit na rizika moznosti zneuziti domen (podvrzeni DNS odpovedi, registrace expirovanych, atd.), upozornit na “default domain name” v konfiguraci routeru a doplit statistikami a grafy ohledne rizik v CZ&SK a nejen tam.

Type of Presentation

Primary author(s) : Mr KUSTEIN, Viktor (Gransy s.r.o.)

Co-author(s) : Mr HORAK, Jan (Gransy s.r.o.)

Track Classification : CSNOG1

Contribution ID : **12** Type : **not specified**

Ochrana proti random subdomain útokům pomocí technologie DNSSEC

Tuesday, 12 June 2018 11:50 (25)

Od roku 2018 mají open-source DNS resolvery novou funkci zvanou agresivní cache (RFC 8198), která efektivně brání některým typům útoků proti autoritativním i rekurzivním DNS serverům.

Během přednášky vyhodnotíme rozvdíl v dopadu random subdomain útoku na DNS zóny, které jsou a nejsou zabezpečeny pomocí technologie DNSSEC. Na datech z měření bude vysvětleno, že pro opetrátory autoritativních serverů je výhodné podepsat zónu pomocí DNSSEC, a že pro operátory resolverů je výhodné provádět DNSSEC validaci.

Type of Presentation

Primary author(s) : ŠPAČEK, Petr (CZ.NIC)

Track Classification : CSNOG1

Contribution ID : **13** Type : **not specified**

Internetworking security

Tuesday, 12 June 2018 15:30 (20)

I při propojování sítí je třeba řešit bezpečnost

GTSM
BFD
BGP FlowSpec
uRPFv3
bezpečnostní nástroje a projekty sdružení NIX.CZ

Type of Presentation

Primary author(s) : POSPÍCHAL, Zbyněk

Track Classification : CSNOG1

Contribution ID : **14** Type : **not specified**

ROV impact simulation & analysis

Tuesday, 12 June 2018 15:50 (20)

Recent work shows that RPKI deployment, currently the most important security extension to the inter-domain routing protocols and amendment of the Internet operation procedures, is severely obstructed by inaccuracies, errors and outdated records in published ROAs. Measurements proved deployment of ROA validation in the Internet is almost non-existing despite the fact that RPKI brings major improvement of Internet routing security without need for large scale and costly hardware upgrades. Attempts to explain reasons that caused slow adoption of the RPKI mechanism describe fear of disconnecting legitimate networks because of erroneous ROA as the leading factor. We utilize NetfFlow data from a real network to simulate ROV and subsequently quantify and analyze traffic that would have been dropped by ROV enforcement. Moreover, we explore methods to distinguish malicious traffic from legitimate one in the stream that would have been lost due to ROV to measure resulting impact of ROV.

Type of Presentation

Primary author(s) : HLAVÁČEK, Tomáš (CZ.NIC)

Track Classification : CSNOG1

Contribution ID : **15** Type : **not specified**

Community infrastructure with vpsFree.cz

Tuesday, 12 June 2018 10:20 (10)

vpsFree.cz is a non-profit association founded in 2008 to host virtual private servers (VPS) for its members. The form of non-profit association means that every member has the right to participate and influence how it is run. Who we are? What we can offer and do for internet community?

Type of Presentation

Primary author(s) : ŠNAJDR, Pavel (vpsFree.cz)

Track Classification : CSNOG1

Contribution ID : **16** Type : **not specified**

Network Fault Isolation

Monday, 11 June 2018 12:05 (25)

NFI (Network Fault Isolation) - Active network monitoring

Most network monitoring relies in the individual network devices themselves telling you that they are healthy or unhealthy via syslog messages, SNMP data, etc. In a Facebook scale network we just can't trust the network devices to accurately report health in all the possible failure cases that may exist. In addition to the standard network monitoring tools, we also actively probe our network with test traffic to ensure it's behaving exactly as we expect. We can now find the network devices that don't even know they are dropping packets even when they exist several layers deep inside the network.

Type of Presentation

Primary author(s) : Mr SHEEHAN, Richard (Facebook)

Track Classification : CSNOG1

Contribution ID : **18** Type : **not specified**

Budoucí nároky videa na sítě

Monday, 11 June 2018 14:20 (25)

Dominantní objem videa konzumovaného diváky se dnes odehrává mimo IP sítě (DVB, satelit, digitální kabelová TV). S fragmentací trhu s videem a s příchodem nových technologií jako je HbbTV nebo ATSC 3.0 můžeme čekat postupné stahování konzumentů videa do IP sítí.

Budou naše sítě připravené na milion TV přijímačů připojených na Internet? Máme k dispozici tipy, triky či černou magii, která nám odloží potřebu masivních investic? Mohou v tom nějak pomoci propojovací centra?

A pokud zbyde čas - vnese masivní distribuce videa skrz IP sítě novou dynamiku do vztahů mezi ISP a jejich propojování.

Type of Presentation

Primary author(s) : KRSEK, Michal

Track Classification : CSNOG1

Contribution ID : **19** Type : **not specified**

Útok skrz (ne)známou vlastnost síťových prvků

Tuesday, 12 June 2018 12:15 (15)

Současné operační systémy síťových prvků nabízejí obrovské množství funkcionality a komunikují skrz širokou škálu protokolů. Přes veškeré jejich přínosy se může někdy stát, že nová funkce se proti nám obrátí a způsobí nám potíže - zejména, je-li takováto vlastnost ve výchozí konfiguraci aktivní. Přednáška pojednává o jedné takové zkušenosti, kdy správcem neznámou a nevyužívanou vlastnost zná a zneužije útočník.

Type of Presentation

Primary author(s) : HEROUT, Tomáš

Track Classification : CSNOG1

Contribution ID : **20** Type : **not specified**

LT: Internetová cenzura v ČR: začatek, skutečný stav a možná evoluce

Monday, 11 June 2018 14:52 (8)

- Legislation in CZ about gambling-related blocking
- Blacklist evolution - from v1 to v7. Gambling with internet Casino. Using PDF as “machine-readable” format.
- Atlas probes on restricted domains. Blacklisting status.
- Possible next steps in CZ. Internet freedom or country-wide Intranet?

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : SAMORUKOV, Oleksii

Track Classification : CSNOG1

Contribution ID : **22** Type : **not specified**

Vizualizace výsledků měření pokrytí

Monday, 11 June 2018 17:55 (25)

Prezentace by se týkala popisu a ukázky nového nástroje, který ČTÚ vyvíjí (testuje) pro účely zpracování a následné vizualizace (i na web. stránkách) naměřených výsledků pokrytí (nejen rádiových parametrů, ale také QoS).

Type of Presentation

Primary author(s) : Mr HOLEK, Karel (ČTÚ)

Track Classification : CSNOG1

Contribution ID : **23** Type : **not specified**

Fighting malware during the DNS resolution

Tuesday, 12 June 2018 13:30 (30)

Most of the malware lifecycle could be observed and even prevented in the DNS traffic. DNS resolver is the ideal place to look for the behavior and eventually act against malicious requests. The presentation will focus on different types of malware requests that can be seen and will discuss experience with fighting malware in a network with approximately hundred thousand of different households in the beginning of 2018. Summary of individual incidents and methods of detection will be presented along with downsides (e.g. application of external Indicators of Compromise) of such approach.
The aim is to give the audience an idea about the number of threats seen in a standard home network and to share experience with challenges in DNS resolution filtering like false positive mitigation. The main presentation structure will follow the malware lifecycle and will present real-life examples, statistics and describe approaches used to solve particular problems.

Type of Presentation

Primary author(s) : Mr ŠEFR, Robert

Track Classification : CSNOG1

Contribution ID : **24** Type : **not specified**

Building 100G DDoS mitigation device with FPGA technology

Tuesday, 12 June 2018 14:30 (30)

The volume of DDoS attacks and their variety grows every year. Since 2016 the largest attacks reached 1 Tbps, effectively disconnecting even well provisioned services from the Internet. CESNET dediced to exploit its expertise in building hardware-accelerated network probes to build its own active device with mitigation capabilities. The device consists of 100 Gbps FPGA network card and a commodity server. The presentation will introduce the FPGA technology in network processing domain as well as outline the concept of the mitigation device. The presentation will also summarize lessons learned during the deployment phase. The rest of the presentation will elaborate on selected mitigation heuristics designed to mitigate volumetric DDoS attacks.

Type of Presentation

Primary author(s) : ZADNIK, Martin (CESNET)

Track Classification : CSNOG1

Contribution ID : **26** Type : **not specified**

Architektura připojení pro kritické služby

Tuesday, 12 June 2018 09:30 (30)

Trvalá dostupnost kritických služeb s širokým uživatelským
dosahem nezávisí pouze na kvalitě implementace koncových aplikací. Zabýváme se dostatečně celou architekturou připojení těchto služeb k síti? Dokážeme udržet jejich dosažitelnost i v případě významných DoS útoků? Obsahem přednášky je zamyšlení se nad řetězcem související síťové architektury a základními aspekty, kterým je vhodné věnovat pozornost.

Type of Presentation

Primary author(s) : Mr KOSNAR, Tomas (CESNET a. l. e.)

Track Classification : CSNOG1

Contribution ID : **27** Type : **not specified**

Měřící infrastruktura pro měření základních parametrů služeb elektronických komunikací

Tuesday, 12 June 2018 11:00 (25)

Český telekomunikační úřad buduje v rámci projektu „Měřící systém elektronických komunikací“ měřící infrastrukturu pro účely kontroly a ověřování vybraných parametrů datových služeb elektronických komunikací poskytovaných koncovým účastníkům v mobilních a pevných sítích. Měřící systém bude disponovat, jak veřejně dostupným nástrojem pro měření aktuální kvality služeb přístupu k síti Internet, tak certifikovanou technologií pro měření. Zároveň budou do infrastruktury implementovány prvky pro zajištění kybernetické bezpečnosti.

Type of Presentation

Primary author(s) : TOMALA, Karel

Track Classification : CSNOG1

Contribution ID : **28** Type : **not specified**

Wi-Fi roaming and open source

Tuesday, 12 June 2018 10:00 (20)

Wi-Fi is now the most common way of connecting to the Internet from user devices. Some of them even use it as the only way to access networks. Because of this it became more important to provide reliable and stable Wi-Fi coverage. In this talk we will be focusing on hostapd, an open source daemon implementing wireless authentication, and its usage in area coverage. Specifically we will be talking about 802.11r and related standards (also known as Wi-Fi roaming).

Type of Presentation

Primary author(s) : KOČÍ, Karel

Track Classification : CSNOG1

Contribution ID : **29** Type : **not specified**

Open-source smerovač na bežne dostupnom hardvéri

Monday, 11 June 2018 13:30 (25)

Témou prednášky bude predstavenie možností postavenia vlastného smerovača na bežne dostupnom hardvéri pomocou open-source softvéru. Aké sú limity dnešných CPU, sieťových kariet a je možné smerovať line-rate n*10Gbps v Linuxe?

Type of Presentation

Primary author(s) : Mr JURENA, Ľubor (skHosting.eu s.r.o.)

Track Classification : CSNOG1

Contribution ID : **30** Type : **not specified**

BGP transport security – do you care?

Monday, 11 June 2018 16:20 (25)

MD5 is insecure. BGP uses MD5 for session authentication therefore BGP is insecure. The internet is broken. Panic!

How many of you use MD5 for BGP sessions? And for what purpose? Isn't MD5 authentication really just a longer form of peer identifier – to avoid accidentally establishing a session with a wrong peer? Does MD5 help in preventing route leaks and hijacks? Does your network allow access to internal BGP speaking nodes from outside of the perimeter? How do you distribute MD5 secrets to your peers? How do you change MD5 secrets without tearing down the BGP session?

TCP Authentication Option has been around for a while. Is anyone aware of TCP-AO? Do any major vendors implement it? Does anyone care? Why not to run BGP over TLS? Or BGP over IPsec? Or BGP over QUIC? Or why not invent a new secure transport for BGP? Sure, that sounds to be a lot of fun, let's do that.
Control plane security has been a special kind of security for a long time. Indeed there are specialty aspects to it as of the layers above relying significantly on the proper operation of the control plane, and often transports used for control planes are not too common ones.

IETF has been working on control plane security for a noticeable period of time, there was a dedicated KARP working group and protocol-specific working groups had their individual initiatives on security aspects. However the world still uses MD5 for BGP. KARP WG got shutdown after a long struggle to produce anything. Is this the question of education, or the lack of it to be precise? Is the problem of peer authentication solved in some other way? Is there a problem at all? Do we need to spend time on spreading the word on what control plane security is and why it is important? Is there a problem at all – given sufficient network operational hygiene and proper network design, do we need control plane security as a separate entity as such? Is there a need for having inbuilt transport security mechanisms into BGP protocol itself?

IETF would like to hear the feedback of operators' community on these topics.

Type of Presentation

Primary author(s) : Mr BAGDONAS, Ignas (Equinix)

Track Classification : CSNOG1

Contribution ID : **32** Type : **not specified**

Vývoj a fungování peeringu v IXP

Monday, 11 June 2018 15:30 (25)

Pohled do minulosti, současnosti a budoucnosti způsobu navazování peeringových relací v prostředí IXP. Možnosti jejich zabezpečení, automatizace, signalizace a kontroly vyměňovaných informací pomocí route serverů a dostupných databází.

Type of Presentation

Primary author(s) : Mr JIRAN, Petr (NIX.CZ)

Track Classification : CSNOG1

Contribution ID : **35** Type : **not specified**

DDoS Beasts and How to Fight Them

Monday, 11 June 2018 09:30 (90)

DDoS threat has been rapidly evolving recently, up to the point when it started to be a community-wide problem. Numerous IoT-related working groups were spawned throughout the last 2 years mostly due to the infamous 1,1Tbps IoT DDoS attack in autumn 2016. Fast-forward 1,5 years, and we see attacks even more disastrous.

This workshop aims at dissecting the DDoS threat. It goes over the ISO/OSI layers, offering a mutually exclusive and collectively exhaustive classification of denial-of-service attacks, a description of what makes them possible, and a set of possible ways to mitigate attacks of any kind, from an ISP perspective.

The workshop is based on a personal experience. It is vendor-agnostic and doesn't cover or promote any solutions available on the market, an attendee is welcome to use this as a guide to build their own.

Type of Presentation

Primary author(s) : GAVRICHENKOV, Artyom (Qrator Labs CZ)

Track Classification : CSNOG1

Contribution ID : **36** Type : **not specified**

BIRD 2.0.x

Monday, 11 June 2018 13:55 (25)

BIRD Internet Routing Daemon is currently the most deployed daemon for router server in IXP environment. It's current stable branch is called 1.6.x. This version has several limitation in AFI/SAFI handling. This talk will introduce the new version branch 2.0.x and show practical differences between those two branches

Type of Presentation

Primary author(s) : Mr FILIP, Ondřej (CZ.NIC)

Track Classification : CSNOG1

Contribution ID : **37** Type : **not specified**

Hromadný sběr anonymizovaných dat pomocí Kolektoru

Monday, 11 June 2018 18:20 (20)

Vytvoření vlastního Kolektoru pro hromadný sběr dat, úskalí a výzvy, cesty kterými jsme se vydali. Co takový sběr obnáší, jaká data jsou sbírána, jak je s nimi poté zacházeno, příklady konkrétního využití.

Type of Presentation

Primary author(s) : Mr SLUGEŇ, Miroslav (Sledovani.TV)

Contribution ID : **38** Type : **not specified**

Routing Security Toolset

Monday, 11 June 2018 15:55 (25)

In this presentation Andrzej will discuss the tools RIPE NCC maintains for routing security: IRR and RPKI.
Network operators face challenges in routing security and we will explain the pros and cons of both tools, their data quality and what the RIPE NCC is doing to optimise the user experience.

Type of Presentation

Primary author(s) : WOLSKI, Andrzej (RIPE NCC)

Track Classification : CSNOG1

Contribution ID : **39** Type : **not specified**

RIPE NCC presentation

Monday, 11 June 2018 11:45 (20)

Type of Presentation

Contribution ID : **40** Type : **not specified**

Opening plenary

Monday, 11 June 2018 11:30 (15)

Type of Presentation

Contribution ID : **41** Type : **not specified**

LT: Bude vaše doména fungovat i v roce 2019?

Monday, 11 June 2018 14:45 (7)

Na den 1. února 2019 je naplánována změna v DNS software. Jste na ni připraveni? Bude vaše doména spolehlivě fungovat i po tomto datu?

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : ŠPAČEK, Petr (CZ.NIC)

Track Classification : CSNOG1

Contribution ID : **42** Type : **not specified**

LT: Quad9DNS : A public benefit service

Tuesday, 12 June 2018 16:17 (8)

Public recursive resolvers are not new. This presentation walks you through what makes Quad9DNS different, and, of true public benefit.

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : GOBURDHAN, Nishal (Packet Clearing House)

Track Classification : CSNOG1

Contribution ID : **43** Type : **not specified**

LT: Network Security Monitoring with Flow Data

Tuesday, 12 June 2018 16:10 (7)

This pitch presentation will highlight how you can leverage flow data (NetFlow/IPFIX/etc.) for anomaly detection & DDoS protection in backbone networks.

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : Mr MINAŘÍK, Pavel (Flowmon Networks a.s.)

Track Classification : CSNOG1

Contribution ID : **44** Type : **not specified**

LT: 400G - don’t get confused with this transceiver generation

Monday, 11 June 2018 16:45 (15)

abstract: Transmission speed of 400G is becoming reality and new challenges for optical and electrical components for high speed systems are emerging as well. PAM4 modulation is one key component for 400G transmission with transceivers. Insights of PAM4 are explained and shown. Packed with this knowledge the new introduced formfactors OSFP, QSFP-DD, SFP56-DD and µQSFP are easier to understand. This will help you to design / build new kind of applications or connections with your networking gear in the field. Avoid pitfalls when designing your racks. Be aware that power consumption and new plugs will also be part of the world of 400G transceivers.

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : Mr WEIBLE, Thomas (Flexoptix GmbH)

Track Classification : CSNOG1

Contribution ID : **45** Type : **not specified**

LT: Pět kroků k elipse

Tuesday, 12 June 2018 16:25 (15)

Prezentace rekapituluje výměnu KSK klíče v doméně .CZ s přechodem na algoritmus ECDSA založený na eliptických křivkách.

Type of Presentation

Ligtning Talk (5 min.)

Primary author(s) : TALÍŘ, Jaromír (CZ.NIC)