Inter-Network Cooperation

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

stole some slides from

Merike Kaeo

cooperation and coordination

- to keep the Internet working
  - we are relying on each other
- it's good to know
  - community
  - point of contact

NOGs

- Network Operations Group is an open forum
  - technology discussions
  - sharing operational best practices
  - compare experience
  - peering coordination
  - establishing personal relationships

medium for NOGs

- mailing-list
  - anyone can subscribe
  - traffic depends on events and topics
- in-person meeting
  - participation fee varies, and costs of transports, accommodations
  - high value

NANOG

- North American Network Operators' Group
  - evolved from the NSFNET "Regional-Techs" meetings in 1994
- Three meetings each year
  - NANOG71, Oct 2017, San Jose
  - NANOG72, Feb 2017, Atlanta
  - NANOG73, Jun 2018, Denver

https://www.nanog.org/

- program
  - 1 day tutorial
  - 3 days plenary
- about 500 attendees
  - from Asia and Europe as well

APRICOT

- Asia and Pacific Operations Conference
  - established in 1996
  - co-located with AP* meetings
- held annually on the last week of Feb
  - APRICOT2016, New Zealand
  - APRICOT2017, Ho Chi Minh City
  - APRICOT2018, Kathmanzu

http://www.apricot.net/

- program
  - 5 days workshop
  - 4 days conference and tutorial
  - 1 day APNIC member meeting
- about 600 attendees

SANOG

- South Asian Network Operators Group
  - established in 2003
- Two meeting each year
  - SANOG 31, Jan 2018, Bangladesh
  - SANOG 32, Aug 2018, Bangladesh
  - SANOG 33, Jan 2018, Thimphu

http://www.sanog.org/

- program
  - 5 days workshop
  - 2 days tutorial
  - 2 days conference
- about 250 attendees

btNOG

- Bhutan Network Operators Group
  - established in 2014
- annual meeting
  - btNOG3, Nov 2016, Thimphu
  - btNOG4, Jun 2017, Thimphu
  - btNOG5.5 (w/ SANOG33), Jan 2018, Thimphu

http://nog.bt/

- program
  - 4 days workshop
  - 1 day conference
- about 120 attendees

JANOG

- Japan Network Operators' Group
  - established in 1997
- local language community - Japanese
- Two meetings each year
  - JANOG41, Jan 2018, Hiroshima
  - JANOG42, Jul 2018, Mie
  - JANOG43, Jan 2018, Yamanashi

http://www.janog.gr.jp/

- program
  - 1 day tutorial + BoF
  - 2 days plenary
- about 500 attendees

BoFs

- birds of a feather(BoF) is a small meeting focused on a specific topic
  - security, peering, and so on
- usually scheduled in advance, sometimes organized on demand

coffee breaks and social events

- to expand relationships
  - business and personal
- to start/manage a project
  - a face-to-face meeting help to step forward things

NOG operation

- independent
  - forms a committee to lead the NOG
- support from cross industry
  - Service Providers
  - Research and Academics
  - Vendors
  - ISOC, NSRC, APNIC, APIA

other upcoming events

- upcoming network-related education or training events
  - http://ws.edu.isoc.org/calendar/

CSIRT

- Computer Security Incident Response Team(CSIRT) provides the incident handling service for its constituency
  - may offer other related services as well

- The first CSIRT - CERT/CC was created in 1988 in response to the Morris worm incident

computer security incident

- Any real or suspected adverse event
- examples:
  - attacks to/from your network
  - compromised host
  - account/information theft
  - spam or IT policy violation

needs for response

- to limit the damage
- to lower the cost of recovery

- an effective response benefits for organizations
  - motivation to have a CSIRT in your organization

The incident handling service

- a single point of contact to receive incident reports
  - provides response and support to the report
  - announcement to disclose information about specific attack/incident
  - feedback to the report/request

What Incidents Should Be Reported?

- Any suspicious activity should be reported
  - This includes suspicious user account behavior, computer system failures or misbehavior, accidental publication of internal email, loss of equipment / account information, etc.
- Reporting methods
  - Internal
    - Online support ticketing system
    - Technical support email
  - External
    - Abuse / incident email contact
    - Public web-based contact form
    - Telephone number specifically for reporting abuse

Information for Reporting An Incident

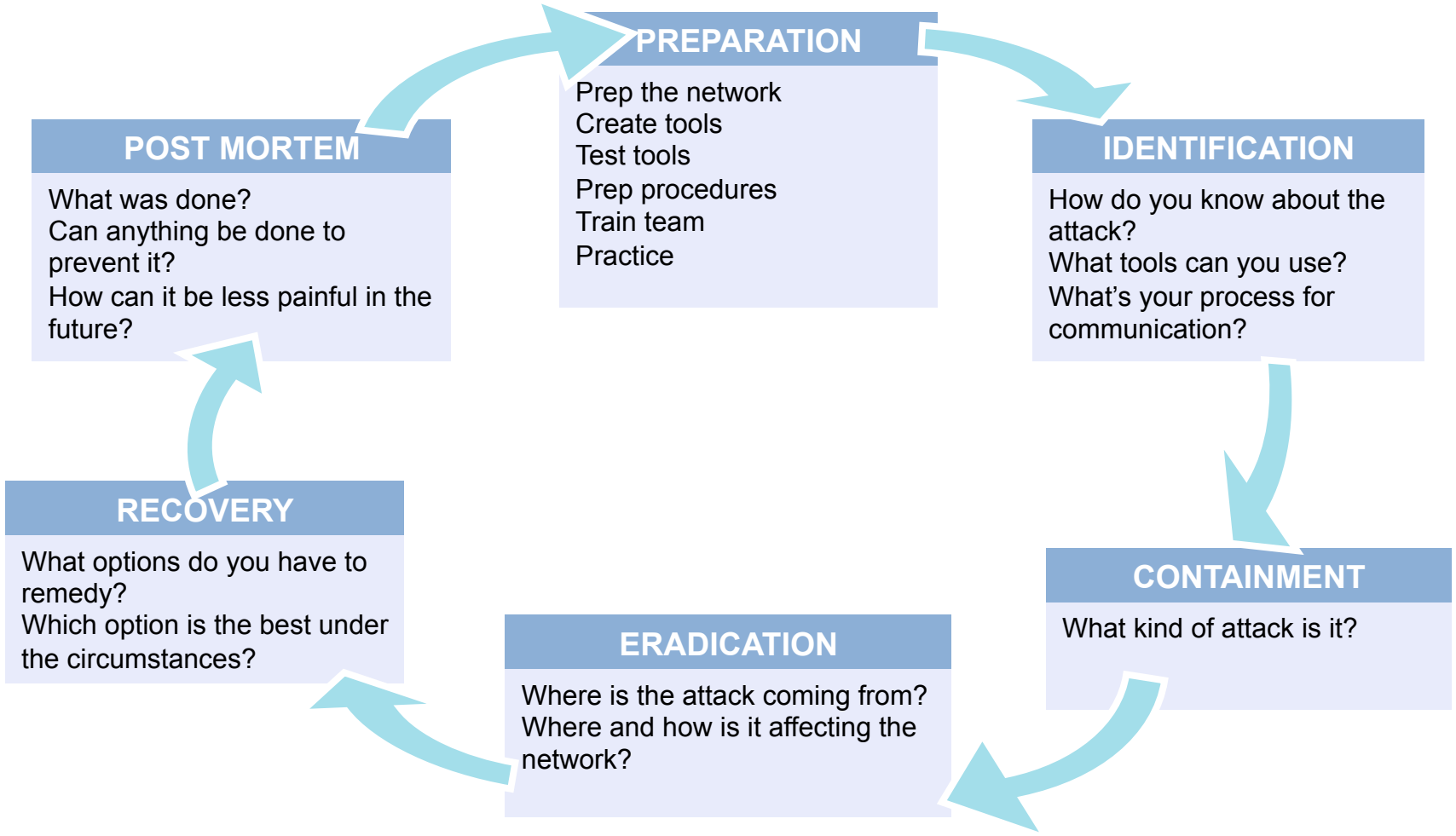
- Date and time of the event
- Description of the event
- Assets that are affected or at risk as a result of the event
- Whether the event is in progress or has concluded
- Actions taken by the party reporting the event
- Informal assessment of the harm or impact to the asset
- Informal assessment of collaterally affected assets
- Data (logs, files, reports) that may assist the CIRT in analyzing the event

Incident Response

- It is always best to have a plan in place before something bad happens
- **DO NOT PANIC!**
- If you set appropriate guidelines now, it will make things a lot easier when a security incident happens

Create a checklist that can be followed when a significant security incident does occur!!

Six Phases of Incident Response



Preparation

- Includes technical and non-technical elements
- Know the enemy
  - Understand what drives the miscreants
  - Understand their techniques
- Create the security team and plan
  - Who handles security during an event? Is it the security folks? The networking folks?
- Harden the devices
- Prepare the tools

Identification

- Goal is to gather events, analyze them and determine whether you have an incident
- Assign Incident Handlers
  - Select a person to handle identification and assessment
  - Empower them to escalate if needed
- Control the Flow of Information
  - Enforce “need to know” policy
  - Tell details to minimum number of people possible
- Create Trusted Communication Channels

How Do You Know You Are Under Attack?

- Understand the details and scope of the attack
  - Identification is not sufficient; once an attack is identified, details matter
  - Guides subsequent actions
- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?
- At the very least:
  - Source and destination address
  - Protocol information
  - Port information

Containment

- Stopping the Damage
  - Prevent attacker from getting any deeper into the impacted systems, or spreading to other systems
- Inform Management
- Notify your local or organizational incident handling team
- Additional 3 phases
  - Short term containment
  - Gathering evidence / backup
  - Long term containment

Short Term Containment

- Try to prevent attacker from causing more damage
- Want untainted evidence
- Some possible actions:
  - Disconnect network cable
  - Pull the power cable (loses volatile memory and may damage drive)
  - Isolate switch port so that system can no longer send/ receive data
  - Apply filters to routers and/or firewalls
  - Change a target's name in DNS to point to a different IP address

Gathering evidence

- This is never easy under pressure
- Hint: Play with these tools and make sure you know how to use them before an incident happens
  - dd for Unix/Linux and Windows
  - Ghost (the latest versions – default is not bit-by-bit so know how to configure)
  - Drive duplicator hardware and write blockers

Long Term Containment

- Once back-up created for forensics analysis the changes for long term containment can begin
- Apply temporary solution(s) to stay in production while building a clean system
  - Patch system
  - Change passwords
  - Remove accounts used by hacker
  - Change file permissions
  - Shutdown backdoor processes used by attacker

Eradication

- Goal is to get rid of any traces on network device(s) that an attack occurred
- Determine how the attack was executed from the gathered evidence
- Restore operating systems and configurations from clean backups
- May require starting from completely wiped systems
- Improve defenses

Recovery

- Goal is to get impacted systems back into production in a safe manner
- Perform system validations
  - Run vulnerability scanners
  - Carefully check application and device logs
- Use network and host-based intrusion detection systems to monitor reoccurrence of attack
- Apply any newly identified mitigation techniques

Post Mortem

- A post mortem will help analyze the event after normal operations has resumed (and people have caught up on sleep)
- Have the meeting soon after the incident passed so everyone has details fresh in their minds
- Do NOT blame anyone for doing something incorrectly
- The primary goal is to address lessons learned and not make the same mistakes next time
- What can you do to make recovery faster, easier, less painful in the future?

building your CSIRT

- mission statement
  - what/how to do
- constituency
  - for whom
- structure
  - budget, position within organization
- relationship with other CSIRTs

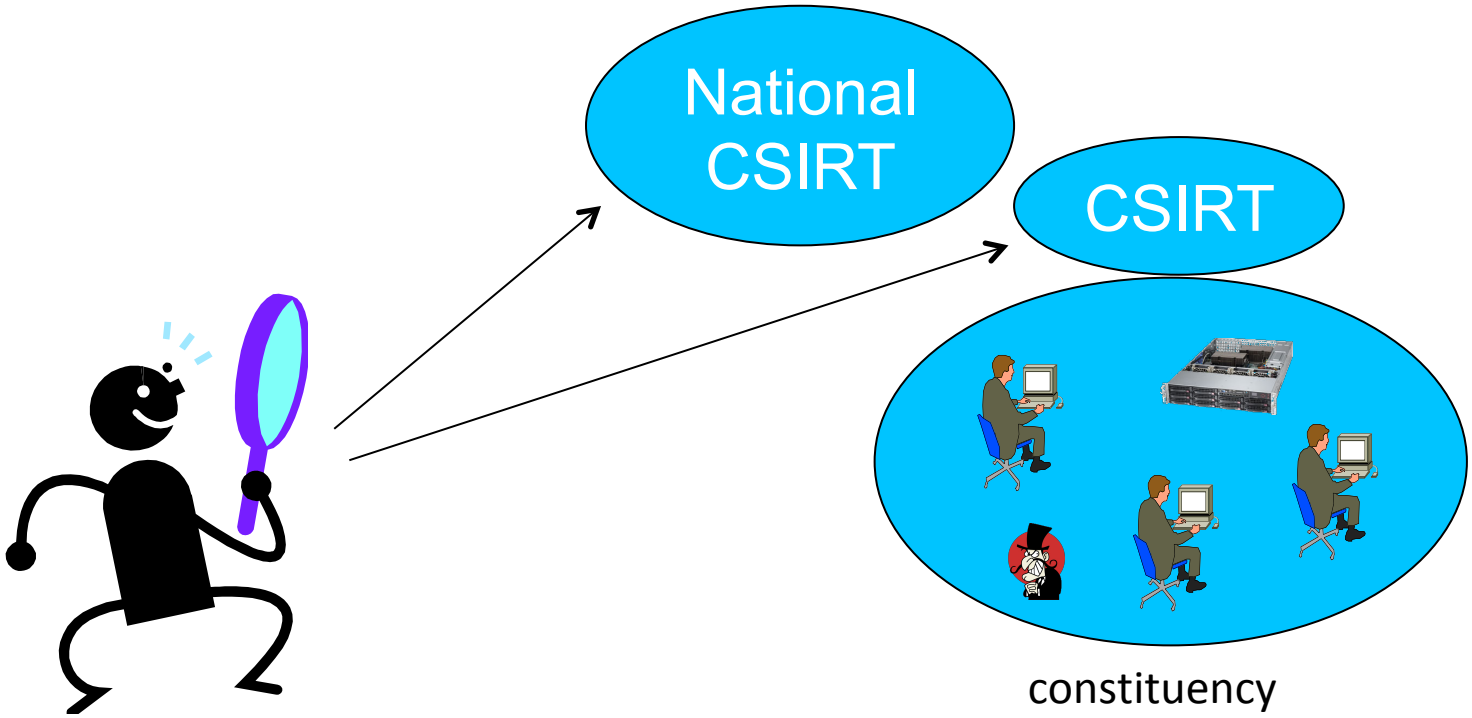
CSIRT types

- National CISRTs
  - a national point of contact to coordinate an incident handling, reduce the number of security incidents in that country
- ISP/xSP CSIRTs
  - provide a secure environment for their customer, and provide response to their customers for security incidents

CSIRT types

- Vendors CSIRTs
  - improve the security of their products
- Enterprise CSIRTs
  - improve the security of their corporation's infrastructure, and provide on-site response for security incidents
- and many more

Point of Contact



Security community

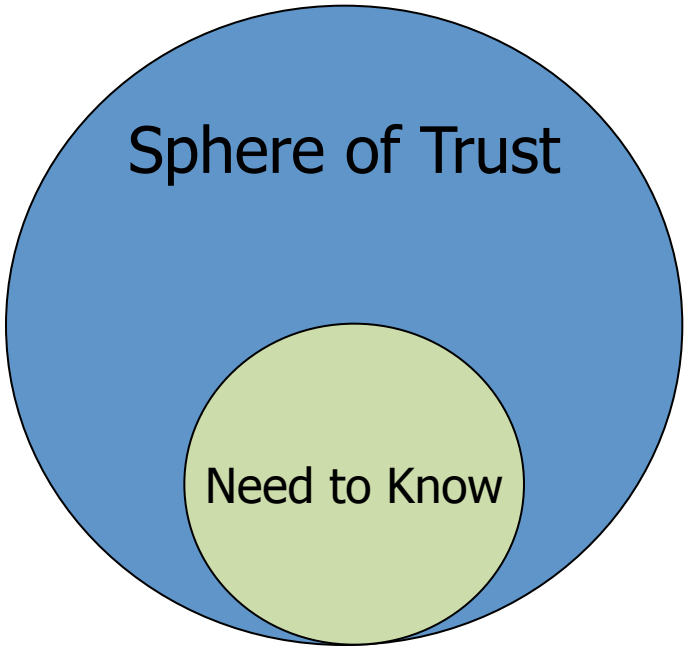
- The following are some example which will provide you a tool and context of the types of groups.
  - Some are open to all
  - Some are personality driven
  - Some are interest driven
  - Some are highly peer vetted

Sphere of Trust

- The community together can be seen as a sphere, realm, zone, of trust.
  - based on chain of Trust

Need to Know in Operation Security

- I trust you. You are someone I can depend on, but you don't really need to know about the details of this incident.
- Not being in a *Need to Know Sphere* does not mean you are not trusted.



Sphere of Action

- You trust someone, but will they be able to do something, be responsive, and/or make something happen?
- Sphere of Action and Chain of Action is a new concept for vetting peers into operational communities.
- Some communities would like to just know something will happen.

I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

Expectation of Action

- “Lurking” is bad behavior on Operational Security Communities.
- There is an expectation of action – where you use the information to do something within your span of control & influence to fight the badness.
  - Collect more data and share.
  - Use your product to act.
  - Use the information to act (i.e. operator)
  - Improve your product or network.
- *Inability to meet expectations erodes trust and your reputation of someone who acts.*

Community's Integrity

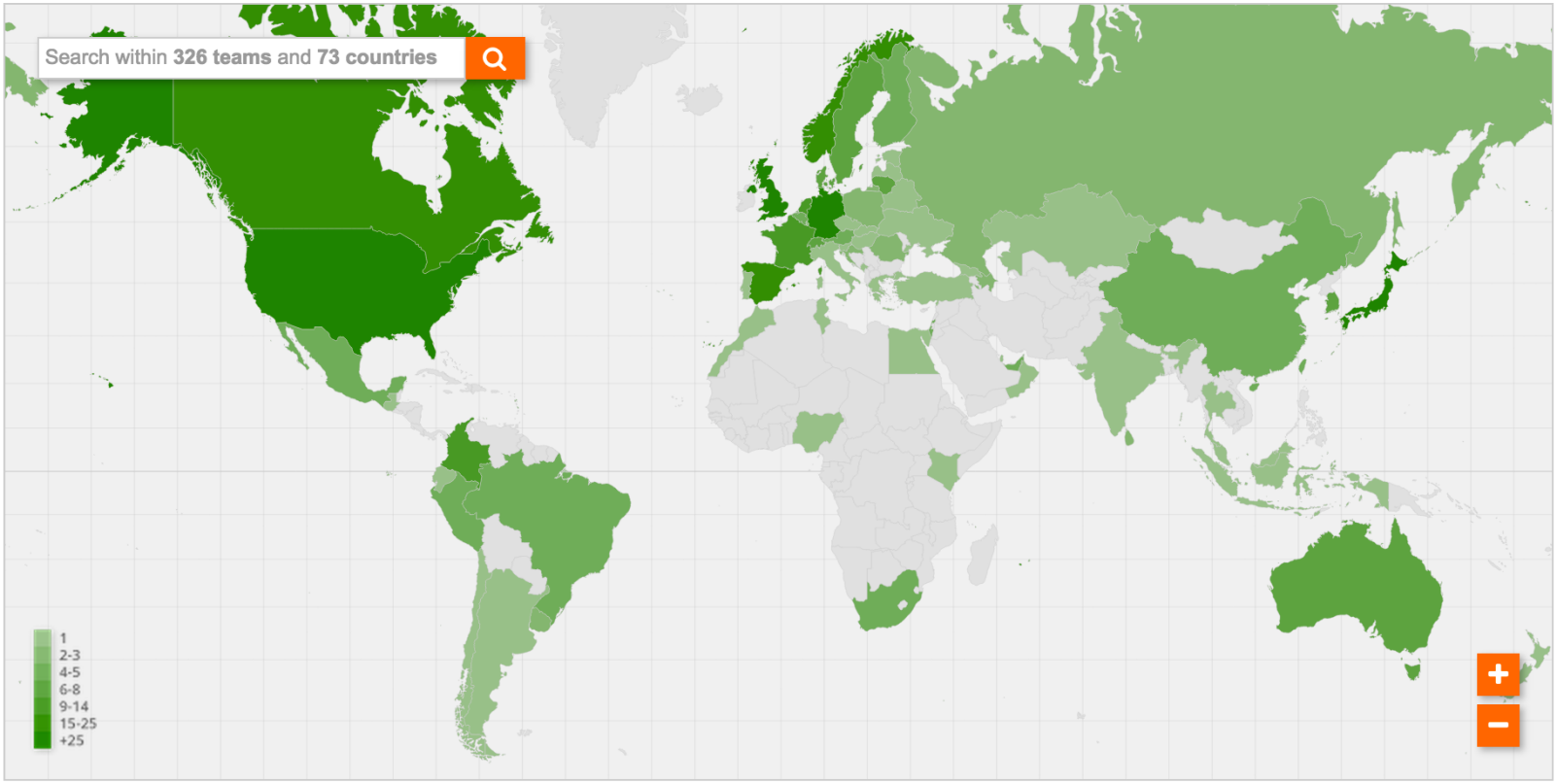
- Maintaining integrity is common sense
- Never **ever** forward information posting within a operational security group without the explicit permission of the person who posted the information
  - Immediate breach of trust
  - Violation of the integrity of the community
- Each individual is accountable to be a steward of the information posted and discussed within the community

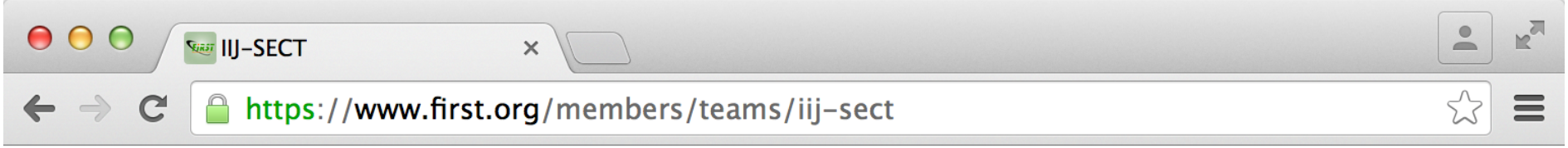
FIRST

- FIRST is international confederation of trusted CISRTs and security teams.
  - Team constituency, rather than individuals
  - Teams from a wide variety of organizations including educational, commercial, vendor, government and military
- Most services are for members only
- https://www.first.org/

FIRST members

Members around the world





Cryptography	
PGP key id	0x2ABB24A5
PGP fingerprint	7381 8456 B4A2 A4C9 A738 0522 9FA4 597F
Team PGP public key	-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.9 (FreeBSD) lQCNAz0lH+sAAAEEAL3X5J3bIfqPL7fzWJ8GAV3G5mEocpRRTsTr2Vwt :J8feAWYKa4Jf+dyLmRk7rEcUOqRNpbo60rJ55XrXQ25KD4amUnkObe+ 'JnjESEjPJPiYAeVBtA1c9AxV/Fna5UYkz+5Q5nhhblCo90cKfvB9yYq .BlJSUogU0VDVCA8c2VjdEBpaWouYWQuanA+iQCVAwUQPSvVfPvB9yYq)AP/ZdNfP4eXOs80vLn4FAJQnEpJV6o1QjGZx07IzGvtqutByJWa7kqTI lUAMWDxtCTbN8i3umFDjjwaOXEuZfv0IQIfi6gY5Ya7JdjsIs67YPKQS /HquTeNeUVhAEHBnvU0rbRTc9T7Zy7UGuvuh30VrJKZq2p+JAJQDBRA9)Rrmb9kBAZ0aA/dQUyN0mrvUA7Q+urUEYu/6a4+5N4XeqXBxROWWc136 :6L6NcDTnK6V0CqnMhEg8bmYsk5zldBLK1VPFA8yUPqxdA7IIQJwyw8GI '5G6copvejZvyfHLR7pWfiEUyE61TeXCUSlmg6nnbyCNMPE221Lz1DHN 'S05dox1ay4slNTtAQFF9wQAwy/AOFVZPwA/bsnAezOaNi6+ahat+xbxI pq2vnqhV7DMvqzeqlm6MEt2nBhtsaOJfvQWhSIdq637HyYQdigzAo9Z 'MOTeHcdBoYBwLNMp+iaawkdzTIuMVoWDr8S23RtxjD+kiO2uwWBW/oFI '2k= :bvV8 -----END PGP PUBLIC KEY BLOCK-----

« back to *Alphabetical list of FIRST Members*

to be a FIRST member

1. Find two existing Full Members for nominating your team ("sponsors")
2. Inform FIRST Secretariat (FSS) that your team wants to join FIRST.
3. Work with your sponsors so they have a thorough understanding of your team
4. Arrange for a site visit by at least one sponsor
5. Provide all the mandatory information requested in support to your nomination (see Section 2.1.2 of the FIRST Membership Process document for details).
6. Provide any additional information requested by FIRST
7. Your sponsor will submit your application (after a 6-month period, at most).
8. Board of Directors will deliver on your specific nomination
9. If application is approved, pay the membership affiliation fee.

https://www.first.org/membership

FIRST events

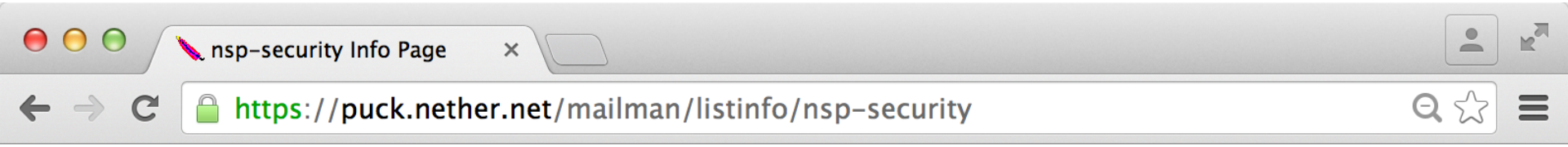
- annual conference
  - every June
  - 29th annual conference
    - San Juan, 11-16 June 2017
  - anyone can attend
- other regional meetings
  - mostly members only

industry based community - ISAC

- Information Sharing and Analysis Center
- Security risks are almost similar in an industry
  - Telecom ISAC
  - Financial ISAC
  - Electricity Sector ISAC
  - ... and many more
- Mostly aiming to protect national critical infrastructures

individual based community

- NSP-SEC
  - https://puck.nether.net/mailman/listinfo/nsp-security
- OPS-TRUST
  - https://openid.ops-trust.net/about



If you'd like to be considered for membership, please provide the following information via email to: nsp-security-owner@puck.nether.net

Name:
E-mail:
DayPhone:
24hrPhone:
INOC-DBA Phone:
Company/Employer:
ASNs Responsible for:
JobDesc:
Internet security references (names & emails):
PGP Key Location:

For Job Description be as detailed and descriptive as possible. After sending the above form via email go to the section below and issue a "subscription" request via the form.

NEW MEMBERS

When a new member requests membership and provides his/her "bio" (as above), once the moderators decide that the potential member has passed their initial review, that person's bio will be sent to the full list. All applications must be accompanied by at least two existing members who will "vouch" for the new applicant (at least one of which must come from outside the same organization). Any existing member will have 48 hours to send reservations about that potential member to the moderators. The moderators promise to review in depth any facts that are raised in regards to any potential new member. The final decision will be left up to moderator discretion based on member input.

RESERVATIONS AND REBUTTAL

Any reservation about an existing member that is sent privately to the -owner list will have all identifying aspects stripped out of the email and forwarded to the potential rejectee for rebuttal. That person will have 72 hours to send a rebuttal before a decision is taken. The moderators of the NSP-SEC list will attempt to take all matters into consideration before rendering a decision.


Operations Security Trust
https://openid.ops-trust.net/about
OPERATIONS SECURITY TRUST
About
Login
Mission
OPSEC-Trust (or "ops-trust") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. OPSEC-Trust carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:
1. sphere of trust;
2. sphere of action;
3. the ability to maintain a "need to know" confidentiality.
OPSEC-Trust (or "ops-trust") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on the malfeasant behaviors which threaten the Internet.
Members:
• will be privy to lists of infected IP addresses, compromised accounts, bot c&c lists and other data that should be acted upon.
• are expected to take appropriate action within their domain of control.
• are expected to contribute data as appropriate and in a fashion that does not violate any laws or corporate policies.
OPSEC-Trust does not accept applications for membership. New candidates are nominated by their peers who are actively working with them on improving the operational robustness, integrity, and security of the Internet.
© OpSecTrust

CVE

- Common Vulnerabilities and Exposures
- Dictionary of common names (ex. CVE identifiers) for publicly known security vulnerabilities
- https://cve.mitre.org/

- We can use a common name to specify a security vulnerability

example: CVE-2015-5986

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5986
- target
  - ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4
- impact
  - vulnerable ISC BIND allows remote attackers to cause a denial of services

ISC BIND release note

- https://kb.isc.org/article/AA-01301/81/BIND-9.10.2-P4-Release-Notes.html

Introduction

:

BIND 9.10.2-P4 addresses security issues described in CVE-2015-5722 and CVE-2015-5986.

CVSS

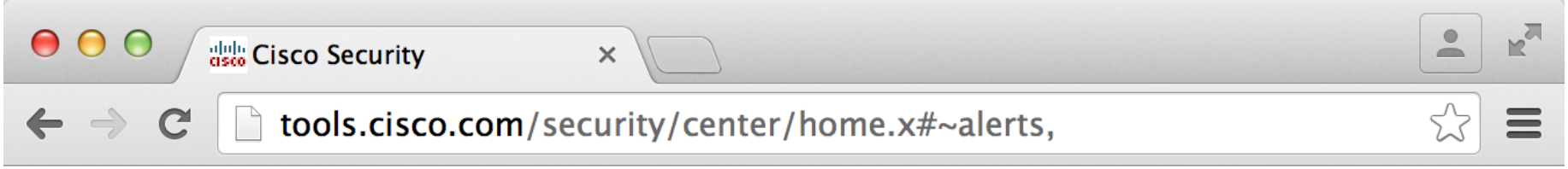
- Common Vulnerability Scoring System
- https://www.first.org/cvss/
  - CVSSv3 is released in 2015
- An open framework for communicating the characteristics and impact of IT vulnerabilities

CVSS Scores

- Base Score
  - technical evaluation
- Temporal Score
  - environmental evaluation
  - proof of concept code/attack code
  - could be changed over the time

CVSS Scores

Security Level	Score
Critical	9 - 10
High	7 - 8.9
Medium	4 - 6.9
Low	0.1 - 3.9
Info	0



Security Highlights | Security Alerts | Upcoming Security Events | Security Blog

View Alerts: --Select--

CVSS Score	Title	Last Updated
7.8/5.8	Linux Kernel UDP Packet Checksum Validation Denial of Service Vulnerability	2015 Sep 16
7.8/5.8	Linux Kernel udp_recvmsg Function Denial of Service Vulnerability	2015 Sep 16
9.4/7.0	GE MDS PulseNET Directory Traversal Vulnerability	2015 Sep 16
8.5/6.3	GE MDS PulseNET Insecure Default Credentials Vulnerability	2015 Sep 16
6.1/5.0	Cisco IOS XE Cisco Discovery Protocol Packet Processing Denial of Service Vulnerability	2015 Sep 16
6.5/4.8	Qemu VNC Display Driver Memory Corruption Vulnerability	2015 Sep 16
7.5/5.5	3S CODESYS Gateway Server Heap-Based Buffer Overflow Vulnerability	2015 Sep 16

Feedback [–]