Assessing and testing communication channels between CERTs and all their stakeholders

Handbook, Document for teachers

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Table of Contents

1 Introduction

Goal

In this exercise, participants will discuss all fundamental concepts of the communication channels between CERTs and their constituents, other CERTs, law enforcement, management, public relations (PR), legal counsel, and all other stakeholders. Special attention is given to communications while under attack, and to the testing of communication channels as a means of safeguarding and improving them.

Target audience

This exercise is useful for incident responders of all experience levels.

Course Duration

4 hours

Frequency

Once for each new CERT member

Structure of this document

	Task	Duration
	Incident start and splitting into groups (plenary)	35 min
	Assignment 1 (in groups)	45 min
	Assignment 2 (in groups)	45 min
	Assignment 3 (in groups)	45 min
	Discussion (plenary)	45 min

2 GENERAL DESCRIPTION

Right from the very start of the CERT community[1] in 1988-89, **communication** between stakeholders was deemed essential for the success of incident response. In fact, the three traditional aspects of information security were essential right from the start: *confidentiality, integrity,* and *availability,* plus another very important one for CERTs: knowing the source of a message and being sure it is from that source. We will refer to that here as *authenticity*.

However, before we come to those, it must be stated that one aspect comes even *before* the four just mentioned: and that is the actual existence of sufficient and trustworthy contact data. After all, without good contacts, CERTs' work would be based on quicksand! These contact points of course need to have been well established in advance; they include such parties as:

[1] http://www.cert.org/encyc_article/tocencyc.html#History

- constituents, both at the operational level through security contacts, as at a higher level (for escalations);
- management, both line management and the top of the organisation (e.g. through a chief information security officer, or CISO);
- press contacts / press office;
- legal counsel;
- vendors and/or vendor-representatives for the most critical information products used in the constituency;
- the CERT community, either through an upstream CERT with good contacts, or by being part of the web of trust yourself;
- national and/or government CERT;
- national security agencies;
- law enforcement;
- other relevant government agencies or contacts;
- relevant support/consultancy parties, e.g. to do scans, or forensics on demand.

Next are the four security aspects presented, in order of priority for CERTs.

1. *Availability*: when communication fails due to saturated, hacked or otherwise sabotaged or failed connections,[2] and if no backup mechanism is in place, then a CERT cannot gain information about the source, character and scope of the attacks; nor can they inform other CERTs or law enforcement about their own findings; and in the case of a spread out constituency, they may find it hard to reach their own constituents.
2. *Confidentiality*: when the heat is on, due to critical incidents, and the stakes are high, communication must be readable only by the intended target, like a fellow CERT, a constituent, or the police. When hacking is going on, one should assume that no connection is secure, and that therefore a communication stream could be tapped or intercepted. Only proper encryption can then safeguard confidentiality. This will only work if the CERT has the public encryption keys of their communication partners.
3. *Integrity and authenticity*: a confidential piece of communication is fine, but the receiver also needs to be sure that the information is untampered with, that is, it remains identical to how it was sent by the originator (*integrity*). And he or she needs to be sure that if the communication claims that it comes from party XY, that indeed it does come from party XY and not from some imposter (*authenticity*). Although these two aspects are not identical, they are usually combined in secure communication (by means of cryptography), and therefore we combine them here too.

Availability is becoming an increasing challenge this decade, because of the fact that TCP/IP is rapidly becoming the protocol of choice for almost all connections.[3] This means that whereas it used to be case that if the Internet failed, the phone would still work, this is no longer guaranteed. Voice over IP (VOIP) is not only used at a local scale, but also backbone providers increasingly integrate all traffic in IP streams. This means that neither is GSM/UMTS voice traffic independent from the Internet anymore, and therefore both landlines and cellular traffic could fail in the case of major outages or attacks. When that happens, most CERTs could right now be essentially isolated. Only a very few teams

[2] Failure may also be due to natural disasters or occurrences like storms, earthquakes, volcano eruptions, landslides etc.

[3] http://techcaliber.com/blog/?p=1100; also private communication of the author in 2011–12 with CTOs of various European backbone providers make clear that TCP/IP over lightpaths is currently the technology of choice. This means that PSTN traffic but also cellphone traffic is all integrated in huge IP streams routed through fibre networks.

have the possibility of using special protected (usually military) networks, bypassing the commercial net. Alternatives have not been seriously discussed or tested yet in the European CERT community, but this will certainly need to happen in the years ahead. Be reminded that in 2004, when the disastrous tsunami happened in the Thailand/Indonesia/India region, the only communication that worked right after the disaster was old fashioned radio,[4] with radio amateurs and professionals establishing and improvising communication paths. Analogue radio as well as packet radio may well be serious options – messenger doves seem less suited.

Confidentiality, *integrity* and *authenticity* pose challenges as well: the increase in challenge is here more a matter of scale and organisation than of a technical nature. After all, the techniques have not really changed in the last few decades – they have merely been improved. Basically, all three aspects are covered by the use of cryptographic techniques based on asymmetrical key-pairs.[5] For secure web traffic, TLS/SSL is used,[6] which is based on the use of so called X.509 client and server certificates: the same are the basis for many sorts of secure tunnels, like the remote login tool SSH and various VPN products.[7] Also, X.509 can be used for secure e-mail based on S/MIME,[8] which is built into all major e-mail products. Some CERTs actually use S/MIME inside their own organisation or community; however, for use between CERTs nationally and internationally, the use of PGP/GPG is pre-dominant, and has been since the early nineties.[9] PGP/GPG is not based on X.509 certificates but instead on PGP key-pairs (same principle, different standard). The main difference between the two is that with X.509 the generation of certificates follows a hierarchical method, whereas with PGP the model is that of a maze: everyone can make their own keys, and trust is only based on the mutual signing of keys, which is the result of a conscious act of both parties involved. This 'trust-exchange' model suits the organisation of the CERT community, as this is more like an organised maze, and not a hierarchical structure. The challenges are mostly organisational, as said above (with the growing number of teams and team members, it is not easy to scale the PGP keymodel) and alternatively it would be at least as challenging to create a certificate infrastructure for the European, let alone the worldwide, CERT community. Additionally, there are some technical challenges too; this is mostly a result of the fact that PGP/GPG is not supported by the main email clients by default. Additional products need to be installed, which sometimes clashes with corporate email policies.

3 EXERCISE COURSE

This exercise is best conducted by a trainer plus a co-trainer.

The exercise allows the trainees to (re)discover all the above aspects and more, during a guided step-by-step discussion, inspired by a fictitious incident that evolves from significant to catastrophical. And not just discover the concepts and ideas, but also think of pragmatic ways to establish, test and maintain working and trustworthy communication channels, also under difficult circumstances.

The fictitious incident is only fed to the trainees piece by piece. For the sake of the trainer it is presented here in its entirety:

[4] http://en.wikipedia.org/wiki/Amateur_radio_emergency_communications and http://www.voanews.com/content/a-13-2005-01-05-voa24-66363817/546509.html

[5] http://en.wikipedia.org/wiki/Public-key_cryptography

[6] http://en.wikipedia.org/wiki/Transport_Layer_Security

[7] http://en.wikipedia.org/wiki/Secure_Shell

[8] http://en.wikipedia.org/wiki/S/MIME

[9] PGP (http://en.wikipedia.org/wiki/Pretty_Good_Privacy) is the original tool, now provided by a commercial company – GPG (or GnuPG, see http://en.wikipedia.org/wiki/GNU_Privacy_Guard) the open source version. Both adhere to the OpenPGP standard (http://tools.ietf.org/html/rfc4880).

Incident scenario

(Piece 1) Shortly after reports of unusually large amounts of DNS query traffic from Canada, backbone network latencies start to climb. ISP network operations managers reach out to CERTs for help in finding the source of the surging traffic on random ports. CERTs of various sorts contact one another, including national and governments CERTs. As the latencies become so high on some places that the SLAs with ISP clients are being violated, ISPs and CERTs contact management and legal counsel to inform them. The first questions from the press come in at the PR/communication departments of ISPs and national CERTs; some CERTs are also contacted directly by the press.
(Piece 2) Then a number of root name servers and gTLD/country-TLD servers appear to be taken down by unknown causes.[10] *Some major neutral internet exchanges also become compromised. Communications, also between CERTs, are seriously hampered, but do still exist, thanks to a lot of improvisation and using trusted parties to relay to others. Given the gravity of the on-going attacks, secure communications are however essential, and prove to be a further challenge in this situation with a seriously damaged communications mesh.*
(Piece 3) Despite the work of many, the ongoing attacks that come from so many sources all over the world are increasingly damaging. Some networks choose to isolate themselves. The remaining traffic worldwide becomes virtually uncontrollable and saturates the Internet. As many backbone links become unusable, most of the phone traffic (including cell phones) dies out too.

The three pieces of the scenario, together with the corresponding three assignments, will be printed separately and given to all groups one at a time. Projecting them will not work as the groups may not all run at the same speed (it is up to the trainer's experience to allow enough flexibility as is needed for the diverse groups) but also keep the overall planning in mind and do not allow the groups to get too much out of sync, for that would lead to some groups not covering all topics.

3.1 Set-up: 20 minutes plenary

The trainer explains to the trainees the goal of the Exercise.

- Discover or rediscover the most important concepts and aspects of communication between a CERT and their various stakeholders.
- Find pragmatic ways to establish, test and maintain working and trustworthy communication channels, also under difficult circumstances.

The trainer continues to explain the set-up used to reach these goals.

- Work in groups of three or four.

[10] See http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers#October_21.2C_2002 , http://erratasec.blogspot.nl/2012/02/no-anonymous-cant-ddos-root-dns-servers.html (especially the footnotes), and http://www.cymru.com/monitoring/dnssumm/: while the set-up of the root name servers is extremely robust, an attack by exploiting vulnerabilities is always feasible; additionally, the gTLD and country TLD servers are probably easier targets.

- Start with the beginning of an incident scenario, and then develop the various concepts and solutions.
- The trainer, assisted by the co-trainer, will continue to visit all groups one after the other and, when concepts/solutions have been developed enough, feed the group the next stage of the incident scenario, allowing the group to discuss more aspects.
- And so on until the time is up – the trainer will seek to help all groups in going through the whole scenario within the set time.
- In each group one trainee is to take notes – and another group member[11] will be asked to present these and/or participate in a guided plenary discussion as the final stage of the Exercise.

[11] If possible the one taking notes should not be the one presenting them – all this to maximise the participation of the trainees.

3.2 Incident start and splitting into groups: 15 minutes plenary

The trainer explains the first piece of the incident scenario.

Piece 1

Shortly after reports of unusually large amounts of DNS query traffic from Canada, backbone network latencies start to climb. ISP network operations managers reach out to CERTs for help in finding the source of the surging traffic on random ports. CERTs of various sorts contact one another, including national and governments CERTs. As the latencies become so high on some places that the SLAs with ISP clients are being violated, ISPs and CERTs contact management and legal counsel to inform them. The first questions from the press come in at the PR/communication departments of ISPs and national CERTs; some CERTs are also contacted directly by the press.

The trainer also explains the first Assignment:

Assignment 1: Discuss, using the incident scenario as thread, the following items.

1. *Quickly establish the CERTs represented in your group and use those as leading examples in the whole Exercise, together with the incident scenario.*
2. *What kind of contacts should your CERT have, like with your constituency of course (two levels, preferably: operational and for escalations), your management (what levels of hierarchy?), etc. Make a list together in the group, not leaving any important party out (so not just the common denominators).*
3. *Discuss if your CERTs actually have those contacts available or if they are really easy to reach.*
4. *Discuss if your CERTs are in touch with your contacts, know them, have worked with them – and if and how that could be important.*
5. *Discuss who are the contacts who need to be available for escalations, which also might mean on Sunday morning or when most colleagues are on holiday – and can you actually reach those contacts when really needed?*

Direct the participants to answer questions, **in brief** – it is up to the trainer to improvise more detail, though it is advised not to go too much into the technical incident detail as this Exercise is about communication concepts, not about technical content.

Then split class into groups of three or four. Learning from group dynamics, two is too small to benefit from the group process and a group of five will result in some people keeping quiet while two or three others do all the talking. If the group has a mix of origins (different organisations, different nationalities) then avoid having people from the same organisation, for instance, in the same group, so that subgroups don't form or the group is not dominated by certain views or ideas. If possible, locate the groups in break-out areas or at least with sufficient distance from one another to avoid auditory interference. Keep these groups until the end of this entire Exercise.

3.2.1 Assignment 1: 40 ± 5 minutes in groups

The trainer and co-trainer split up the groups between themselves and then attend to their groups. The groups have five items to discuss and each item could take between five and ten minutes, with the exception of Item 2, which could take 10–15 minutes. This means that the trainers need to gently steer the groups if they take too much time on items. If the group is very fast instead, the trainer could entertain some discussion with the group, ask additional questions or give suggestions: there is plenty to discuss here, and if a group fails to see if they will need some help.

Somewhere between 35 and 45 minutes into the exercise, each group can be led into the next Assignment (see next paragraph). Note that this does not have to happen at the same time for each group; in fact, this won't be possible, as the trainers will be touring their groups and each group will

have its own dynamic. This 'out-of-sync' approach continues until the plenary at the end of this Exercise: it does require synchronising on-the-go between the two trainers, to make sure that the groups do not go out-of-sync by more than 15 minutes.

3.2.2 Assignment 2: 40 ± 5 minutes in groups

The (co-)trainer explains the second piece of the incident scenario:

Bit 2:
Then a number of Root Name Servers and gTLD/country-TLD servers appear to be taken down by unknown causes.[12] Some major neutral internet exchanges also become compromised. Communications, also between CERTs, are seriously hampered – but do still exist, also thanks to a lot of improvisation, and using trusted parties to relay to others. Given the gravity of the on-going attacks, secure communications are however essential, and prove to be a further challenge in this situation with a seriously damaged communications mesh.

And he/she explaines the second Assignment:

Assignment 2: Discuss, using the incident scenario as thread, the following items.

1. Confidentiality: when the heat is on, due to critical incidents, and the stakes are high, communication must reach only the intended target, like a fellow CERT, a constituent or the police. When hacking is going on, one should assume that no connection is secure. Discuss in your group how your CERTs have solved this issue in regards to communication with their points-of-contact (the ones you discussed before!), and how there may still be blind spots in this regard. Also bear in mind a situation like in the incident, where some of your usual communication partners may not be reachable anymore and therefore you will need to relay through others – how do you do that securely?
2. Integrity and Authenticity: an exclusive piece of communication is fine, but the receiver also needs to be sure that the information is **whole**, that is, identical to how it was sent by the originator (in other words, integrity). And he/she needs to be sure that if the communication claims that it comes from party XY, that indeed it does come from party XY and not from some imposter (in other words, authenticity). Discuss among yourselves, following on the discussion of confidentiality, how you have solved (or not solved) this issue for your points-of-contact.
3. DNS failure: this is an issue of availability of communication. DNS failure is unlikely to easily happen, but is not unthinkable. When it happens, the Internet still functions, but name resolution stops working. You will need to rely on IP numbers instead. Discuss in your group how your CERTs are prepared for such an event – and what should be done to be prepared.

The trainer and co-trainer proceed as before. Each item of the Assignment is expected to take 10–15 minutes. After 35-–5 minutes, the groups are led into the last Assignment (see next paragraph). Again, the groups are allowed to go out-of-sync, but preferably by no more than 15 minutes.

3.2.3 Assignment 3: 40 ± 5 minutes in groups

The (co-)trainer explains the third piece of the incident scenario:

[12] See http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers#October_21.2C_2002 , http://erratasec.blogspot.nl/2012/02/no-anonymous-cant-ddos-root-dns-servers.html (especially the footnotes), and http://www.cymru.com/monitoring/dnssumm/ : while the set-up of the Root Name Servers is extremely robust, an attack by exploiting vulnerabilities is always feasible – additionally, the gTLD and country TLD servers are probably easier targets.

Bit 3:

Despite the work of many, the on-going attacks that come from so many sources all over the world are increasingly damaging. Some networks choose to isolate themselves. The remaining traffic worldwide becomes virtually uncontrollable and saturates the Internet. As many backbone links become unusable, most of the phone traffic (including cellphones) dies out too.

[Note : if a very technically savvy group wants to embark on a discussion on the technical feasibility of this scenario, remember that this Exercise is not about that. Although the authors of this Exercise are convinced that this is feasible, you could easily bypass this debate by adding the detonation of a small nuclear bomb in the atmosphere near to a critical infrastructure point, which would literally burn out all non-military communication by means of EMP. The authors would rather that you avoid the use of such heavy ammunition, as it detracts from the likelihood of the scenario, but it is there for you to use if it helps you reach the goals of this Exercise.]

And the third Assignment:

Assignment 3: Discuss, using the incident scenario as thread, the following items:

1. Availability: when communication fails due to saturated, hacked or otherwise sabotaged connections, and if no backup mechanism is in place, then a CERT cannot gain information about the source, character and scope of the attacks; nor can they inform other CERTs or law enforcement authorities about their own findings; and in the case of a spread out constituency, they may find it hard to reach their own constituents. Discuss in your group how your CERTs have taken this possibility into account, how they plan for it, and what they do when it happens, in these two situations:
    - most of the phonesystem (landlines and cellphones) still works;
    - most or all of the phone system (including cellphones) is down too.

   Be aware that the latter is not unlikely at all these days, with the advent of VOIP not just on local loops and inside organisations, but also on the backbone level, where providers are more and more tunneling **all** traffic through IP. Usually only military teams (but possibly also national and/or government teams) can use special, protected networks, which would hopefully still work in cases of emergency. What other means are there?

2. Testing communications: Discuss, bearing all you learnt in this Exercise, the case for the testing of communications. This includes the regular testing of things like:
    - points-of-contact;
    - cryptography used;
    - fallback mechanisms when DNS fails;
    - fallback mechanisms when the Internet fails;
    - fallback mechanisms when the Internet and phones fail.

   How do you test it? What to bear in mind? Could this be implemented as a regular test? Or as part of regular fire drills?

The trainer and co-trainer proceed as before. Each item of the Assignment is expected to take roughly 20 minutes. After 35–45 minutes the groups are led into the break (see next paragraph). Again, the groups are allowed to go out-of-sync, but at this stage by no more than 15 minutes.

3.2.4 Break: 25–40 minutes (plenary)

The first group to break will have about 40 minutes break, the last group to break (15 minutes later) will have 25 minutes – all others will be in-between. Thus, the plenary break leads all groups back into sync, and onto the last part of the Exercise.

The trainer and co-trainer prepare the plenary discussion together during the break.

3.2.5 Discussion: 30–45 minutes (plenary)

The trainer and co-trainer lead a discussion of the lessons learnt from this exercise. In each group, notes have been taken, to facilitate this discussion. It is advised that the trainers simply follow all above Assignments in order for the discussion. This can most easily be done by asking group #1 to discuss Assignment 1, item 1. Then plenary – asking other groups to comment and steering the discussion with suggestions if needed. Then on to group #2 – Assignment 1, item 2, etc., starting again with group#1 after the last group has had its turn. Give special attention to **availability** and **testing** in the discussions. Invite the trainees to actively **use** the results of this exercise in their teams, to enhance awareness and invite them to plan more proactively on points-of-contact, availability and security of communication, and how to regularly test all facets of the CERT's communication channels.

4 EVALUATION METRICS

Evaluating the results of this Exercise, the trainer should take into consideration the class's understanding of these key concepts:

- the necessity of an extensive and accurate list of points-of-contact (see Introduction for a non-exhaustive list) which will also work under duress (e.g. escalations outside office hours);
- safeguarding the availability of communication to the points-of-contact at least, also when DNS fails, when the Internet fails, and when also the phones fail;
- safeguarding the security of communication to the points-of-contact at least; security meaning confidentiality, integrity, and authenticity (availability is already treated in the previous bullet item);
- knowledge of applicable communication cryptography like GnuPG/PGP, PGP/MIME, S/MIME (based on X.509 instead of PGP);
- understanding of infrastructural threats to communication, like the non-availability of DNS, and the increasing reliance on IP for both VoIP and cellphone traffic;
- availability of main sources of CERT contact information, like the TI database, FIRST website, ENISA CERT info, IRT and abuse contact info from the RIPE database (and ARIN etcetera).

5 REFERENCES

European CERTs contact info:

- TI database: https://www.trusted-introducer.org/teams/
- ENISA CERT inventory: http://www.enisa.europa.eu/activities/cert/background/inv
- IRT objects in RIPE IP-number database: http://www.ripe.net/data-tools/db/faq/irt-faqs; as an example try this query: https://apps.db.ripe.net/search/query.html?searchtext=192.87.106.101&flags=B&sources=RIPE_NCC&grssources=&inverse=&types=#resultsAnchor and click on the 'mnt-irt: irt-SURFcert' which yields https://apps.db.ripe.net/whois/lookup/ripe/irt/irt-SURFcert.html (all contact info for the team called SURFcert)

Teams outside Europe:

- FIRST worldwide membership info: http://www.first.org/members/map
- Asia-Pacific teams cooperating in APCERT: http://www.apcert.org/about/structure/members.html
- North-American IP number registry: http://whois.arin.net/ui and as an example query for 128.103.200.35 and find http://whois.arin.net/rest/net/NET-128-103-0-0-1/pft and subsequently click on the Abuse info for Harvard University http://whois.arin.net/rest/poc/ABUSE3331-ARIN.html
- For Latin America use http://lacnic.net/cgi-bin/lacnic/whois and search for abuse-c fields
- For Africa use http://www.afrinic.net/en/services/whois-query similarly to Latin America
- For Asia-Pacific use http://www.apnic.net/apnic-info/whois_search/about similarly to Latin America

Documentation:

- ENISA *Good Practice Guide for Incident Management* http://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management (e.g. pp. 18–19, 22, 36, 52, 67–68)
- *Handbook for Computer Security Incident Response Teams (CERTs)* http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm (e.g. p. 102–106)
- General ENISA information for CERTs : http://www.enisa.europa.eu/activities/cert

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu