Date of Submission: 5/14/04

Personal Information

Primary Speaker Name: Tony Arcieri

Speaking on Behalf of: PDTP.org

Has the speaker spoken at a previous DEFCON? No

Presentation Information

Name of Presentation: PDTP – The Peer Distributed Transfer Protocol

How much time does your presentation require? 50 minutes

Is there a demonstration? No

Are you releasing a new tool? Yes

Are you releasing a new exploit? No

Is there audience participation? No

What are your equipment needs?

Will you require more than 1 lcd projector? No

Will you require wireless internet access? No

Will you require wired internet access? Yes

Will you require a white board? No

Are there any other special equipment needs that you will require? No

Detailed Outline:

1. Brief introduction to PDTP and the problem domains being addressed
2. Overview of existing technologies, such as FTP, HTTP, and BitTorrent, and their respective strengths/drawbacks
3. Overview of how these respective problems, such as mirror selection and file tampering, are addressed in PDTP
4. Technical overview of system components
5. Technical overview of protocol design
    - A) Transaction format
    - B) Peer protocol
    - C) Datagram classes
    - D) Input validation concerns of protocol design
6. Overview of file transfer process
    - A) FTP/mirror-like behavior
    - B) BitTorrent-like behavior
    - C) Alternatives to TCP for piece transfers
    - D) Firewall concerns
7. PDTP network designs
8. libpdtp design/implementation and API overview, licensing
9. Server component design/implementation, licensing
    - A) Scalability features (constant time event monitoring)
    - B) Native operating system support features, VFS monitoring
    - C) Server framework overview
    - D) Unit testing overview
    - E) Memory debugging overview
10. Cryptographic file validation overview (DSS signatures/x.509 certificates)
11. Rich directory listings/metadata overview
12. Search system overview
    - A) Underlying search protocol
    - B) Tracker networks
13. IETF draft overview/IANA recognition (and hopefully timeline to RFC adoption)
14. Future development projects (Skyfire client application, licensing)
15. Getting involved/project management overview
16. Official release of all Milestone 1 PDTP components/conclusion
17. Q&A session

Supporting documentation may be found at the following URLs:
http://pdtp.org/
http://pdtp.org/faq.php
http://pdtp.org/protocol.php
http://pdtp.org/networks.php

Abstract:

Despite decades of evolution, Internet file transfer is still plagued with problems to which formalized solutions are either inadequate or nonexistent. Lack of server-side bandwidth often renders high demand content inaccessible (which we affectionately refer to as the Slashdot effect). When the ability of a single server to provide content is exceeded, manual mirror selection is often utilized, providing an unnecessary and often problematic experience for end users. No formalized cryptographic mechanism exists for preventing tampering of files located on a particular server, and consequently malicious individuals have managed to place trojans in the releases of many high profile open source applications.

The Peer Distributed Transfer Protocol (PDTP) aims to solve all these problems. PDTP can either function with a network of servers providing content directly to clients, or can provide BitTorrent-like “download swarming” by forcing clients to participate in file transfers. PDTP includes built-in mechanisms to prevent file tampering through the use of the Digital Signature Standard, and is able to automatically verify that a given file has been signed by a DSA key with a complete x.509 certificate check to ensure a given certificate can be trusted. PDTP also provides a UDP-based decentralized search mechanism which, unlike current systems such as FastTrack, Gnutella, or FreeNet, does not consume undue bandwidth or system resources, all while removing legal liability for content indexing from the central services being utilized as entry points to the search system.

Supporting File(s):

Additional files/materials? Yes

Type of file(s): Protocol specification as an IETF working draft in RFC2629 XML format, text, HTML (Note: Not yet complete!)

Speaker's Bio(s):

Tony Arcieri is a system administrator and programmer for the Pielke Research Group and Colorado Climate Center at Colorado State University. He has also contributed to a number of open source projects, including authoring the Ogg Vorbis plugin for XMMS, the cdcd and gdcd X11 CD player applications, and various contributions to other projects such as the Subversion version control system and the FreeBSD operating system.

Transfer of Copyright

I warrant that the above work has not been previously published elsewhere, or if it has, that I have obtained permission for its publication and that I will promptly supply DEFCON Communications, Inc. with wording for crediting the original publication and copyright owner.

If I am selected for presentation, I hereby give DEFCON Communications, Inc. permission to duplicate, record and redistribute this presentation; including, but not limited to, conference program, conference CD, video, audio, hand outs(s) to the conference attendees for educational, on-line and all other purposes.

I, Anthony Arcieri, have read the above and agree to the Transfer of Copyright.

Agreement to Terms of Speaking Requirements

If I am selected to speak, I understand that I must complete and fulfill the following requirements or I will forfeit my honorarium:

1) I will submit a completed (and possibly updated) presentation, a copy of the tool(s) and/or code(s), and a reference to all of the tool(s), law(s), Web sites and/or publications referenced to at the end of my talk and as described in this CFP submission for publication on the conference CD by noon PST, July 7, 2004.

2) I understand if I fail to submit a completed presentation by July 7, 2004, I may be replaced by an alternate presentation or may forfeit my honorarium.

3) I will include a detailed bibliography as either a separate document or included within the presentation of all resources cited and/or used in my presentation.

4) I will complete my presentation within the time allocated to me - not running over the time allocation.

5) I understand that DEFCON will will provide at least 1 lcd projector, 1 screen, microphone, and video switch box. I understand that I am responsible for providing all other necessary equipment, including laptops and machines (with VGA output), to complete my presentation

6) I will submit, within 5 days of the completion of the conference, any updated, revised or additional presentation(s) or materials that were used in my presentation but not included on the conference CD or conference proceedings.

I, Anthony Arcieri, have read the above and understand and agree to the terms as detailed in the Agreement to Terms of Speaking Requirements.

Agreement to Terms of Speaking Remuneration

1) I understand that I will be responsible for my own hotel and travel expenses.

2) I understand that DEFCON will issue one payment per presentation.

3) I understand that in order to be paid, I must provide a valid name and snail mail address. US citizens will be paid with a company check. Non-US citizens will be paid via money order or company check.

4) I understand that the name and address that I provide to the onsite speaker liason is where the payment will be sent.

5) I understand that I will be paid $200 USD, 30 days from the end of the conference, after I have completed my presentation. I may choose to waive my $200 speaking fee in exchange for 3 DEFCON Human badges.

6) I understand that should my talk be determined to be unsuitable (eg a vendor or sales pitch, a talk on the keeping of goats, etc) after I have presented, that I will not receive an honorarium.

I, Anthony Arcieri, have read the above and understand and agree to the terms as detailed in the Agreement to Terms of Speaking Remuneration or I will forfeit my honorarium.