第14回FreeBSDワークショップ

佐藤　広生 <hrs@FreeBSD.org>

東京工業大学/ FreeBSD Project

2016/1/25

http://people.allbsd.org/~hrs/sato-FBSDW20160125.pdf

開催背景

- **日本国内の＊BSDユーザ活動を活発化させましょう**
  - 月1回、東京近辺で定期的な会合を
  - 講演を聞くだけでなく、話を持ち寄って双方向に議論しましょう

http://people.allbsd.org/~hrs/sato-FBSDW20160125.pdf

本ワークショップの進行

- 19:00〜19:45　自己紹介＋話題にしたいトピック
- 19:45〜20:00　休憩
- 20:00〜20:50　ライトニングトーク
- 20:50〜21:00　最近のSA + α

意見は自由に発言ください！

http://people.allbsd.org/~hrs/sato-FBSDW20160125.pdf

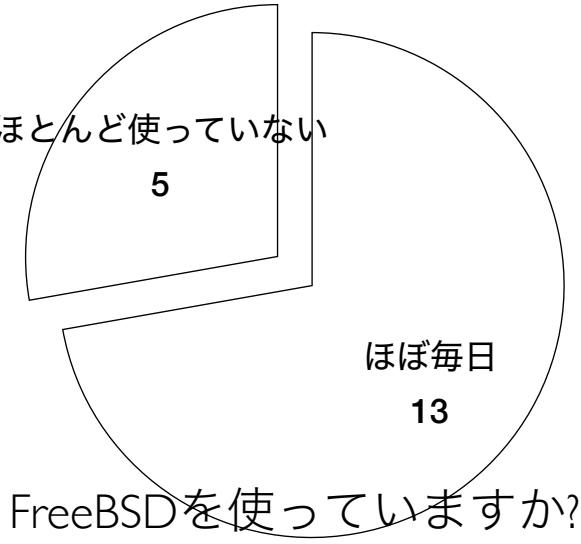
オーガナイザの自己紹介

- 名前：佐藤 広生
  - FreeBSD コアチームメンバ、リリースエンジニア(2006-)
  - FreeBSD Foundation 理事(2008-)
  - その他の＊BSD／オープンソース関連の活動いろいろ
  - 東京工業大学助教(2009-)

自己紹介タイム

- 名前（所属）
- 開発者 or 利用者
- 興味がある／話題にしたい内容

をどうぞ



FreeBSDを使っていますか?

今回の出席者内訳：新規5名、再参加者13名

メモ

メモ

最近の話題

- **EN/SA (1/25)**
- FreeBSD-SA-16:01.sctp

ICMPv6 Header Type: Dest Unreachable Code: 0	IPv6 Header Next header: SCTP	SCTP Header (12 bytes)

SCTPパケットがdest unreachとなった時、戻るICMPv6パケットに含まれるSCTPヘッダは上記のようにカプセル化される。ICMPと異なり、ICMPv6は原因パケットの大部分を含んでいることに注意。

- このSCTPヘッダが12バイトより短かった場合にnull pointer deref が発生する

http://people.allbsd.org/~hrs/sato-FBSDW20160125.pdf

最近の話題

- FreeBSD-SA-16:07.openssh
  クライアントにあるローミング機能が悪用可能。
  サーバ側に細工が必要で、ホスト認証は影響を受けない（これを使ってMITM攻撃はできない）。
- クライアントが秘密鍵をstdio.h関数群を使って読み、その後に領域をfreeするため、メモリ上に秘密鍵が残っている。
- ローミング機能の穴を突いてメモリにアクセスできる
- UseRoming no を .ssh/config に。

最近の話題

- FreeBSD-SA-16:07.openssh
  OpenSSHを7.0に上げた人は、DSA鍵が無効になっているので注意。
- DSAの危険性

$\mathrm{signature(r, s)}$

SHAハッシュ関数

$$r = g^k \mod p \mod q$$
$$s = k^{-1}\left(H(m) + x \cdot r\right) \mod q$$

元メッセージ　秘密鍵

最近の話題

- FreeBSD-SA-16:07.openssh
  OpenSSHを7.0に上げた人は、DSA鍵が無効になっているので注意。
- DSAの危険性

$\mathrm{signature(r, s)}$

SHAハッシュ関数

random nonce

$$r = g^k \mod p \mod q$$
$$s = k^{-1}\left(H(m) + x \cdot r\right) \mod q$$

元メッセージ　秘密鍵

最近の話題

$\mathrm{signature(r, s)}$

SHAハッシュ関数

random nonce

$$r = g^k \mod p \mod q$$
$$s = k^{-1}\left(H(m) + x \cdot r\right) \mod q$$

元メッセージ　秘密鍵

違うメッセージmA, mBを同じ鍵とkで署名

$$S_A = k^{-1}\left(H(m_A) + x \cdot r\right) \mod q$$
$$S_B = k^{-1}\left(H(m_B) + x \cdot r\right) \mod q$$

http://people.allbsd.org/~hrs/sato-FBSDW20160125.pdf

最近の話題

$\mathrm{signature(r, s)}$

SHAハッシュ関数

random nonce

$$r = g^k \mod p \mod q$$
$$s = k^{-1}\left(H(m) + x \cdot r\right) \mod q$$

元メッセージ　秘密鍵

引き算してみる

$$S_A - S_B = k^{-1}\left(H(m_A) - H(m_B)\right)$$
$$k = \left(H(m_A) - H(m_B)\right) / \left(S_A - S_B\right)$$
$$x = \left[S_A \cdot k - H(m_A)\right] / r$$

k, x が計算できる

最近の話題

- DSAの危険性
  - random nonceが予測可能な場合、
    署名結果から秘密鍵が漏えいする。
  - PRNGの信頼性が低く、DSA署名時に
    同じ値が使われていたりするとアウト
  - CVE-2008-0166(DSA-1571-1)
    - DebianにふくまれていたOpenSSLパッケージの
      PRNGの周期が32,768しかなかった問題

告知

- FreeBSDワークショップ（ほぼ月一回）
  （次回は2月18日）
- AsiaBSDCon 2016
  2016/3/10-13
  東京理科大学 森戸記念館
  飯田橋駅から徒歩5分、東京理科大学の施設