It’s the people, stupid.
Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

This document describes HTCPCP, a protocol for controlling, monitoring, and diagnosing coffee pots.
Serverless Systems
Useless Systems
RULES

CHANGE VS. MORE OF THE SAME

THE ECONOMY, STUPID

DON'T FORGET HEALTHCARE
Change vs. more of the same.
The people, stupid.
Don’t forget malware.
The Downward Spiral of Cynicism

Developers

- That can’t happen.
- That doesn’t happen on my machine.
- That shouldn’t happen.
- Why does that happen?
- Oh, I see.
- How did that ever work?
• That never worked.
• Must be the network.

@jschauma
The Downward Spiral of Cynicism

- It’s not the network.
- Probably a bug in the OS.
- Oh, ok. DNS.
- Don’t monkey around with /etc/hosts.

Developers

SysAdmins

SRE

@jschauma
The Downward Spiral of Cynicism

Developers

SysAdmins

SRE

BOFH

- An African or European swallow?
- You don’t know what you’re doing.

@jschauma
The Downward Spiral of Cynicism

Developers

SysAdmins

Infosec

SRE

BOFH

- That’s not how you do this.
- Nobody knows what they’re doing.

@jschauma
The Downward Spiral of Cynicism

- Developers
- SysAdmins
- Infosec
- New Yorkers
- SRE
- BOFH

- What? I don’t care, keep walking. Don’t talk to me.
- Seriously, don’t stop in the middle of the street. I will cut you.

@jschauma
The Downward Spiral of Cynicism

Developers
SysAdmins
Infosec
New Yorkers
SRE
BOFH
New York Infosec SysAdmin
Showing 351,777 available code results

- robocoder/phpvh – SqlInjectionGet.php
  - Showing the top two matches. Last indexed on Oct 3, 2015.
  ```php
  <?php
  mysql_query("SELECT * FROM table WHERE field='$_GET[query]'");
  ?>
  ```

- ewilded/SCARY – xss_and_sql_false_positive2.php
  - Showing the top two matches. Last indexed on Oct 1, 2015.
  ```php
  <?php
  $b="SELECT ".$_GET['id'];
  $b=htmlspecialchars($b);
  mysql_query($b); # SQL
  ?>
  ```
$ cat .bash_history
cc -Wall setuid.c
./a.out /etc/sudoers
ls -l /etc/sudoers
ls -l a.out
sudo chown root a.out
ls -l a.out
sudo chmod 4755 a.out
ls -l a.out
./a.out /etc/sudoers
mysql -u root --password=w34kSawz
sudo chown daemon a.out
ls -l a.out
./a.out /etc/sudoers
clear
vi access.c
cc -Wall access.c
ls -l a.out
ls -ld
rm a.out
ls -l a.out
cc -Wall access.c
$
<table>
<thead>
<tr>
<th>T</th>
<th>Key</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INC0570977: [Security Issue S0] Credentials exposed on GitHub</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S0-201</td>
<td>[S0] Credentials Available on GitHub</td>
</tr>
<tr>
<td></td>
<td>IT-12560</td>
<td>[Security Issue - S0] Github Information Disclosure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Security Issue S0] Credentials Available on GitHub</td>
</tr>
<tr>
<td></td>
<td>IT-2716</td>
<td>[Security Issue S0] Credentials exposed on github</td>
</tr>
<tr>
<td></td>
<td>IT-2727</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td></td>
<td>IT-2703</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td></td>
<td>V-4300</td>
<td>[Security Issue S0] Credentials exposed on GitHub (PSI)</td>
</tr>
</tbody>
</table>
Jan Schaumann
@jschauma

Password requirements: 30 chars, upper/lower/special chars, numbers, ancient egyption hieroglyp; reset question: your mother's maiden name?

RETWEETS 19  LIKES 16

7:36 PM - 21 May 2015
How not to be seen
Changing other people’s habits is a wicked problem.
Long-lived SSH Connections
Firewall / ACLs / idled(8) ...
Reverse SSH tunnel
Privkeys on prod
cron(8) initiated callbacks
...

Velocity NY 2016
Amplification of perceived risk

Risk
  - Voluntary
    - Self controlled
      - Pure – rock climbing
    - Diminished control
      - Applied – driving
    - No control
      - Cycling
  - Impersonal
    - Nature Economy
      - Plane Train
      - Mount Etna
    - Benign
      - Mobile phone masts
    - Profit Motivated
      - GMOs
    - Malign
      - Al Qaida

Acceptability of risk

Risk Amplification

Velocity NY 2016  https://is.gd/80zCWX  @jschauma
Why we take our shoes off at the airport.
#Infosec: Silicon Valley’s TSA

- Little Bobby Tables
- Secrets on GitHub
- XSS

NSA-proofing TLS cipher spec

Velocity NY 2016 @jschauma
Security is not a value.
Nobody cares about security.
Nobody cares about security. That is neither incompetence nor malice, it’s pragmatism.
People driven defense

Effective defense

“sophisticated”

“military grade encryption”

“NSA-proof”

“even more cyber”

“cyber”

Vendor Crap “Security Appliances”
dedicated, motivated, human adversaries
Ceci n’est pas un hacker.
dedicated, motivated, human adversaries
Velocity NY 2016
Safety, not (just) security.
A system is *secure* if it protects the user when used correctly.

A system is *safe* if it protects the user even when used *incorrectly*. 

Velocity NY 2016  
@jschauma
INSERT CORRECTLY
ON THIRD TRY
If your reaction is “well, not like that”, you have a poka-yoke problem.

Fix that.
The most convenient / intuitive way to use your application must be the *safest* way to use your application.
Users will not change default settings.
Users will not change default settings. 
(Unless a less secure option is available.)
Failure must not lead the user to change their default settings.
Failure must not lead the user to change their default settings.

Safety overrides must be temporary.
Your applications, services, standards, etc., must age gracefully.
Poká-yoke software & systems

- safe defaults
- safe failure mode
- automated, regular, unattended updates
- puts usability ahead of ‘security’
- encourages desired behavior
- builds / strengthens safe habits
- follows the users’ desire path
Change vs. more of the same

- avoid the downward spiral of cynicism
- your users, developers, engineers, ... are not stupid; they’re trying to get their job done
- focus on realistic threats, not high-profile security theater
- understand that your attackers are motivated, dedicated, human adversaries

The people, stupid.

- security is not an end-goal
- build safe applications & services
- understand your users’ desire paths
- Poka-yoke Go!

Don’t forget malware.
“Fundamentally, the problem isn’t about security. It’s about people.”
- Bill Clinton (not quite)

Thanks!
Image Attributions

- Monty Python, Paul Townsend [https://flic.kr/p/nVFKH5](https://flic.kr/p/nVFKH5)
- Downward spiral, Davo Sime [https://thenounproject.com/term/downward-spiral/589704/](https://thenounproject.com/term/downward-spiral/589704/) [https://creativecommons.org/licenses/by/3.0/us/](https://creativecommons.org/licenses/by/3.0/us/)
- Mouse, Martin Driver, [http://wallpapersafari.com/w/UzqRxW](http://wallpapersafari.com/w/UzqRxW)