

Data Leaks Found on the Net

John Kristoff

jtk@depaul.edu

+1 312 362-5878

DePaul University
Chicago, IL 60604

What am I talking about?

- Data I've stumbled upon in my net travels
 - Data that some people would classify as private
- Mosts data leaks are not that serious
 - At least for large communities of interest
 - They are usually easily to fix and avoid
- There are lots of leaks and they are everywhere
 - I can only show you a small sample
- I am not advocating security by obscurity

Leaks exist and persist

- Search engines can find a lot of data leaks
- Creativity can find the rest
- Mirrors
 - Essentially a backup of data found on the net
- Caches
 - Temporary backups of data found on the net
- Newsgroup/mailing list archives
 - User postings backed up on the net

Things found in a search engine

- Passwords to protected sites and files
- PGP key rings (private keys too? ... you bet!)
- Intrusion detection and penetration testing reports
- Web server usage and statistics information
- Temp., test and member-only files and directories
- Source code and configuration information
- Pager and cellular phone numbers
- Default server installations – probably vulnerable

A search engine may miss...

- Directories listed in `http://<site>/robots.txt`
- Some things found in HTML source code
- File types other than HTML
- Dynamically generated pages and URLs

In your deFACEment

From: adma@defaced.alldas.de
To: alldas-defaced-edu@defaced.alldas.de
Subject: [alldas-defaced-edu] vivien.astro.cornell.edu defaced by AIC

Defaced website: vivien.astro.cornell.edu
Defaced-by: AIC

IP: 132.236.7.140

Mirror URL: <http://defaced.alldas.de/mirror/2001/11/01/vivien.astro...>

NMAP Output: <http://defaced.alldas.de/?did=25165&xid=1>

Webserver: Apache/1.3.9 (Unix) mod_perl/1.21

OS guess: Solaris

- Up-to-the-minute-custom *hack me* list?
- Uhhmm... kinda YEAH!
- ...Yikes!

Hi. I've been hacked. You?

```
Nov 8 16:29:58.427 cst: %SEC-6-IP-ACCESSLOGP: list 123 denied tcp  
192.0.2.1(1655) -> network.host(80), 1 packet
```

```
192.0.2.1 - - [08/Nov/2001:16:32:16 -0600] "GET  
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404  
313
```

... repeated ad nauseum...

- Looks like the source has a worm...
- It must be vulnerable, because...
- Its announcing it to the whole world!
- ...Doh!

Not-so-private IP addressing

```
Return-Path: <joe.schmoe@example.com>
Delivered-To: jtk@aharp.is-net.depaul.edu
Received: (qmail 14246 invoked from network); 22 Mar 2001 16:08:14 -0000
Received: from merlin.depaul.edu (140.192.1.9)
    by aharp.is-net.depaul.edu with SMTP; 22 22 Mar 2001 14:08:14 -0000
Received: from l4duppx2.example.com (l4duppx2.example.com [192.0.2.1])
    by merlin.depaul.edu (8.10.2/8.10.2) with ESMTP id f2MFeCk09419
    for <jtk@depaul.edu>; Thu, 22 Mar 2001 09:40:12 -0600
Received: (from noaccess@localhost)
    by l4duppx2.example.com (8.9.3/8.9.3) id KAA00627
    for <jtk@depaul.edu>; Thu 22 Mar 2001 10:08:07 -0600 (CST)
X-Authentication-Warning: l4dupfw42.example.com: noaccess set sender to
    <joe.schmoe@example.com> using -f
Received: from lintng1.example.com(10.20.68.64) by l4dupfw42 via smap
    (V2.1+anti-relay+anti-spam)
    id xmaa00461; Thur, 22 Mar 01 10:07:03 -0600
Received: by lintng1.example.com (Lotus SMTP MTA v4.6.6 (890.1 7-16-1999)
    id 86256a17.005888ac ; Thu, 22 Mar 2001 10:06:58 -0600
X-Lotus-FromDomain: EXAMPLE
From: "Joe Schmoe" <joe.schmoe@example.com>
To: jtk@depaul.edu
Message-ID: <239832911.239821a99.00@lintng1.example.com>
Date: Thu, 22 Mar 2001 10:10:49 -0600
Subject: NAT sucks
```

Public router security

```
router>show access-list
Standard IP access list 1
    permit 192.0.2.0, wildcard bits 0.0.255.255
    deny any
Standard IP access list 2
    deny 224.0.1.39
    deny 224.0.1.40
    deny 239.0.0.0, wildcard bits 0.255.255.255
    permit any
Standard IP access-list 3
    deny 224.0.1.39
    deny 224.0.1.40
    permit any
Standard IP access list 4
    deny any
Standard IP access list 5
    permit any
Standard IP access list 6
    permit 192.0.2.0, wildcard bits 0.0.255.255
    permit 192.0.2.0, wildcard bits 0.0.0.255
    deny any
Standard IP access list 7
    permit 192.0.2.0, wildcard bits 0.0.1.255
    deny any
---More---
```

More public router fun

- `show ip access-list`
 - Shows ACL hits
- `show log`
 - Lots of good detailed information
- Open UDP/TCP sessions
 - BGP sessions, syslog server, ntp server, etc.
- Ability to view interfaces and ACLs applied
- Ping, traceroute, telnet, ttcp and other tools

One of my personal favorites

-- Security Alert Consensus --
Number 03 (00.14)
Thursday, March 30, 2000
Network Computing and the SANS Institute

Welcome to SANS's distribution of the Security Alert Consensus.

Edit page at <http://www.sans.org/sansaddr?hashid=SD324426a9LsLfibQ6x>
to change your preferences or any other personalized information.

...

- Hmm... what if we search for "sansaddr"?
- Surely no one would forward that email...
- ...Whoopsie!

Don't just cover your ASCII

...

```
Here is a representative example of one of the packets, taken with tcpdump:
09:39:07.148532 65.197.243.120.2557 > mercury.80: S [tcp sum ok]
      263101219:263101219(0) win 8192 <mss 1380> (DF) (ttl 106,
      id 39171, len 44)
0x0000      4500 002c 9903 4000 6a06 b6eb 41c5 f378
0x0010      839c 0803 09fd 0050 0fae 9b23 0000 0000
0x0020      6002 2000 027b 0000 0204 0564 0000
```

...

- Hmm... what is mercury, the IP is hidden.
- Or is it... hmm... review RFC 791 for decoding...
- We decode 0x83 0x9c 0x08 0x03 and...
- ...Doops!

Another obfuscated try

...

We also see those tcp 21536 packets. Did you also observe UDP 37852 packets ? We are trying to determine if they are due to similar problem.

Capture of packets (anonymized) follow :

```
08:09:30.529936 194.133.58.129.55 > XXX.XXX.142.42.37852: udp 10 (ttl
53, id 46545)
```

```
4500 0026 b5d1 0000 3511 6ff4 c285 3a81
XXXX 8e2a 0037 93dc 0012 0bb5 0000 0000
0000 0000 0000 0000 3335 3420 456e
```

...

- First 16 bits of destination IP obfuscated
- But... 16 bit checksum (0x6ff4) is there!
- Reverse packet through the checksum routine...
- ...Doops, Doops!

Cold hard cache

- Browser history, cookies and temporary files
 - Library and other public hosts
- Temporary and swap files
 - What can we find with a simple `strings`?
- Google cache
 - Very, very handy, unless you've screwed up

Stupid application tricks

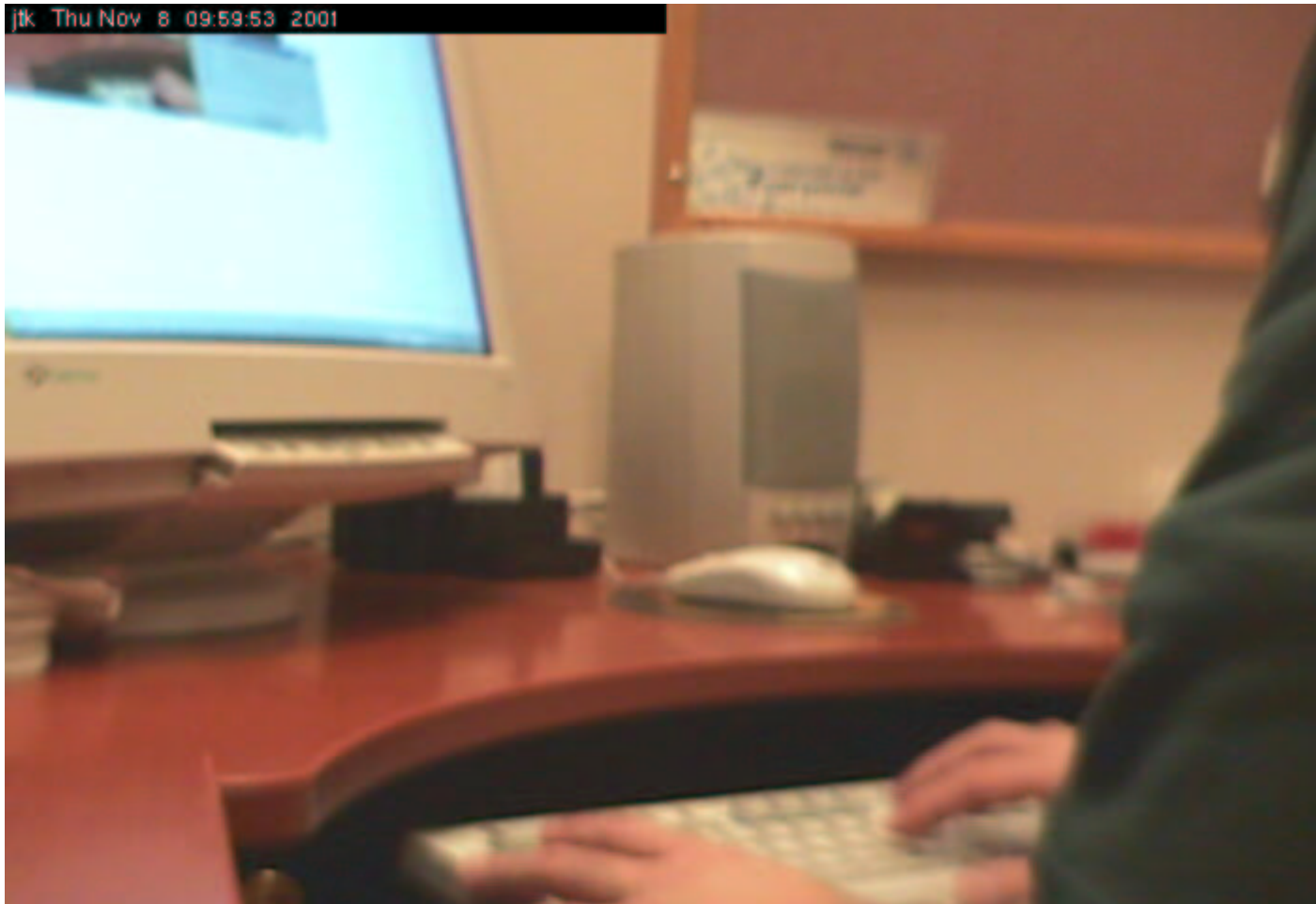
"Due to the way Microsoft Excel, Microsoft PowerPoint, and Microsoft Word for Windows use OLE for file storage, documents created in these programs may contain extraneous data from previously deleted files [...]"

Wire-mess

The screenshot shows the Network Stumbler application window. The interface includes a menu bar (File, Edit, View, Options, Window, Help), a toolbar with various icons, and a left-hand sidebar with a tree view containing 'Channels', 'SSIDs', 'bobsucks', 'networkcna', 'tsunami', and 'Filters'. The main area displays a table of detected networks. The status bar at the bottom indicates 'Ready', '3 APs active', and 'GPS: Disabled'.

MAC	SSID	Name	C...	Vendor	Type	WEP	SNR	Signal+	Noise-
● 0230650...	bobsucks		11	Apple	Peer		5	-77	-98
● 0040964...	tsunami		11	Cisco (Aironet)	AP	Yes	7	-82	-99
● 0040963...	networkcna		1	Cisco (Aironet)	AP	Yes	24	-61	-99

Next generation data leaks



Avoiding data leaks

- Know what your hosts and applications are doing
- Avoid spyware applications if at all possible
- Be wary of spying providers and hosts too
 - Are they tracking your DNS usage?
 - Watching your IP-to-IP conversations?
- Use and demand end-to-end encryption
- Look for leaks about yourself and your organization
- Don't assume others will safeguard your data