Embracing the “Hack”
A better strategy for team-Defense
thanks!
Widespread attacks are now the exception, not the norm

- Server-side exploits
  - IIS, SQL, DCOM
- Productivity app exploits
  - Office, Adobe Reader
- Browser-based exploits
  - Internet Explorer, Adobe Flash, Java, ActiveX controls

Exceptions exist, e.g. Wannacry

Windows XP SP2 Ships
  - Firewall on-by-default & DEP
Windows Vista Ships
  - ASLR
Office 2010 Ships
  - DEP, ASLR, & Protected View
Edge ships
  - Sandbox, ASLR, DEP, CFG, etc

https://www.youtube.com/watch?v=PjbGojhnBZQ
Widespread attacks are now the exception, not the norm.
“Your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents”

- Brian Snow
Most enterprises are not safe

"SECURE 100"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

https://www.slideshare.net/astamos/appsec-is-eating-security
Most enterprises are not safe

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

```
FORTUNE 500
```

```
TOASTED 400
```

Everybody Else
“Back to Basics”

“Management Buy-In”

“Think like an Attacker”
“Back to Basics”

“Management Buy-In”

“Think like an Attacker”
Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021

Cybersecurity Ventures' 2019 Cybersecurity Market Report sponsored by Secure Anchor

- Steve Morgan, Editor-in-Chief
Sausalito, Calif. - Jun. 10, 2019

The cybersecurity market is continuing its stratospheric growth and hurtling towards the trillion dollar mark that we originally predicted on May 31, 2017.

Cyber Security Market Worth Over $140 Billion in 2019

Published: Mar 19, 2019 12:14 p.m. ET

Mar 19, 2019 (AB Digital via COMTEX) -- Global Cyber Security Market: Demand Analysis and Growth Forecast

As per the findings by a newly compiled business study by IndustryARC, the
“Management Buy-In”

https://www.youtube.com/watch?v=2WtW237U-y4
“Back to Basics…”

“Management Buy-In”

“Think like an Attacker”
Thought Leader @thoughts

blah blah blah blah BACK TO BASICS blah blah blah blah
blah blah blah blah blah blah blah blah blah blah blah blah blah!

#ThoughtsLed

1 Retweet
A kind of survivorship bias
If it were simple, it would have been done already
Improving the Security of Your Site by Breaking Into it

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@porcupine.org

Introduction

Every day, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, there are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins, because by their very nature they are much harder to detect.

CERT. SRI. The Nic. NCSC. RSA. NASA. MIT. Uninet. Berkeley. Purdue. Sun. You name it, we've seen it broken into. Anything that is on the Internet (and many that isn't) seems to be fairly easy game. Are these targets unusual? What happened?

Fade to...

A young boy, with greasy blonde hair, sitting in a dark room. The room is illuminated only by the luminescence of the C64's 40 character screen. Taking another long drag from his Benson and Hedges cigarette, the weary system cracker telnets to the next faceless "mail" site on his hit list, "guest -- guest", "root -- root", and "system -- manager" all fail. No matter. He has all night... he pencils the host off of his list, and tiredly types in the next potential victim...

This seems to be the popular image of a system cracker. Young, inexperienced, and possessing vast quantities of time to waste, to get into just one more system. However, there is a far more dangerous type of system cracker out there. One who knows the ins and outs of the latest security auditing and cracking tools, who can modify them for specific attacks, and who can write his/her own programs. One who not only reads about the latest security holes, but also personally discovers bugs and vulnerabilities. A deadly creature that can both strike poisonously and hide its tracks without a whisper or hint of a trail. The uebercracker is here.

Why "uebercracker"? The idea is stolen, obviously, from Nietzsche's ubermensch, or, literally translated into English, "over man." Nietzsche used the term not to refer to a comic book superman, but instead a man who had gone beyond the incompetence, pettiness, and weakness of the everyday man. The uebercracker is therefore the system cracker who has gone beyond simple cookbook methods of breaking into systems. An uebercracker is not usually motivated to perform random acts of violence. Targets
1993 to 2019
Trend Micro Threat Defense Challenge

Are you ready to defend against cybersecurity threats? Come and participate in the Threat Defense Challenge!

Join our security experts for a hands-on learning experience in a real-world scenario to simulate a cyberattack. Learn to "think like a hacker" and then respond to and defend valuable assets. Whether you are a novice or a skilled security professional, this experience has something for everyone!

Play alongside your peers and compete in teams to run cyberattacks in a controlled environment. Premium prizes will be awarded to the team who gains the most points.

August 22, 2019 at 9:00 am

REGISTER TODAY >
Here's what's wrong with think like an attacker: most people have no clue how to do it. They don't know what matters to an attacker. They don't know how an attacker spends their day. They don't know how an attacker approaches a problem. Telling people to think like an attacker isn't prescriptive or clear.
Learning the wrong lessons from Offense
@haroonmeer

https://t2.fi/2017/02/05/haroon-meer-keynote-2016/
Tight Feedback Loops
Attackers write Code
Why Software Is Eating The World

By MARC ANDREESSEN

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its PC business in favor of investing more heavily in software, where it sees better potential for growth. Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised me. But both moves are also in line with a trend I’ve observed, one that makes me optimistic about the future of the American and world economies, despite the recent turmoil in the stock market.

In short, software is eating the world.

More than 10 years after the peak of the 1990s dot-com boom, a dozen or so new Internet companies like Facebook and Twitter are sparking controversy in Silicon Valley. These rapidly growing private market valuations, and the occasional successful IPO. With scars from the dot-com bubble still fresh in the investment community, the question everyone is asking, “Isn’t this just a dangerous new bubble?”

I, along with others, have been arguing the other case. (I am co-founder and general partner of the firm Andreessen-Horowitz, which has invested in many of these tech companies.) The answer is yes, but also no. Yes, the valuations are high. But there is a significant difference between consumer Internet companies and the dot-com companies of the early 2000s.

In an interview with WSJ’s Kevin Delaney, Groupon and LinkedIn investor Marc Andreessen insists that the recent popularity of tech companies does not constitute a bubble. He also stressed that both Apple and Google are undervalued and that “the market doesn’t like tech.” In an interview with WSJ’s Kevin Delaney, Groupon and LinkedIn investor Marc Andreessen insists that the recent popularity of tech companies does not constitute a bubble. He also stressed that both Apple and Google are undervalued and that “the market doesn’t like tech.”
Most enterprises are not safe

“SECURE 100”
- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

“TOASTED 400”

Everybody Else

https://www.slideshare.net/astamos/appsec-is-eating-security
Most enterprises are not safe

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

Fortune 500

“SECURE 100”

“TOASTED 400”

Everybody Else

What are they missing?
- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

https://www.slideshare.net/astamos/appsec-is-eating-security
they build infrastructure
Beyond the (Beyond the Hype)

“Why your threat model is probably wrong”

(haroon meer - thinkst applied research)
(3) Professionals & Toolchains

- Professionals are more than just the latest 0day

- Almost more than anything else, Professionals build tool-chains
  - Bug Hunters will have complex tool chains to minimize bug hunting pain,
  - Professional attackers will have complex tool chains to funnel in and out of your network
Example #2: Timing & Camels

- A simple beginning.. \texttt{oneTime.py} *
- A generalized Solution ? \texttt{squeeza.rb}
- Introducing Camels ? \texttt{reDuh} *
- ...

Ever Expanding Tool Chains..
NSA Leaks
(not just 0days)
Canarytokens by Thinkst

What is this and why should I care?

Web bug / URL token

Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered, like: URL within Dropbox

Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

Web bug / URL token

haroon@thinkst.com

Reminder note when this token is triggered, like: URL within Dropbox

Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

- Web bug / URL token
- haroon@thinkst.com
- USENIX Demo - Desktop

Create my Canarytoken

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

Your Web token is active!
Copy this URL to your clipboard and use as you wish:

http://canarytokens.com/articles/feedback/2grufU7my71fwrn9b

Remember, it gets triggered whenever someone requests the URL.

If the URL is requested as an image (e.g. `<img src=""`) then a 1x1 image is served.
If the URL is surfed in a browser than a blank page is served with fingerprinting Javascript.

Ideas for use:
- In an email with a juicy subject line.
- Embedded in documents.
- Inserted into canary webpages that are only found through brute-force.
- This URL is just an example. Apart from the hostname and the actual token (the random string), you can change all other parts of the URL.

https://canarytokens.org/generate
Canarytoken triggered

An HTTP Canarytoken has been triggered by the Source IP 34.242.239.31.

Basic Details:

<table>
<thead>
<tr>
<th>Channel</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>2019-08-14 00:18:12</td>
</tr>
<tr>
<td>Canarytoken</td>
<td>iru3u7my71fwm0b9r5iy3y3k</td>
</tr>
<tr>
<td>Token Reminder</td>
<td>USENIX Demo - Desktop</td>
</tr>
<tr>
<td>Token Type</td>
<td>web</td>
</tr>
<tr>
<td>Source IP</td>
<td>34.242.239.31</td>
</tr>
<tr>
<td>User Agent</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36</td>
</tr>
</tbody>
</table>

Canarytoken Management Details:

- Manage this Canarytoken [here](#)
- More info on this token [here](#)

Powered by [Threat Canary](#)
Canarytokens by Thinkst

What is this and why should I care?

Select your token

Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered.

Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered, like: Hostname in /etc/hosts of server X

Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

DNS token

haroon@thinkst.com

Reminder note when this token is triggered, like: Hostname in /etc/hosts of server X

Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.


https://canarytokens.org/generate
Canarytokens by Thinkst

What is this and why should I care?

Your DNS token is active!
Copy this hostname to your clipboard and use as you wish:

st7bpmos3hm2xi1psvb81u.canarytokens.com

Remember, it gets triggered whenever someone performs a DNS lookup of the hostname.

The source IP address shown in the alert is the DNS server, not the end user.

Ideas for use:

- Include in a PTR entry for dark IP space of your internal network. Quick way to determine if someone is walking your internal DNS without configuring DNS logging and monitoring.
- Leave in a .bash_history, or .ssh/config, or ~/servers.txt
- Use as a extremely simple bridge between a detection and notification action. Many possibilities, here’s one that tails a logfile and triggers the token when someone logs in:
  ```bash
tail -f /var/log/auth.log | awk '/Accepted publickey for/ { system
```  
- Use as the domain part of an email address.

https://canarytokens.org/generate
host:~ attacker$ host st7hjpcmcos3hz2xi5pzvb81u.canarytokens.com
host:~ attacker$ host st7hjpmcos3hz2xi5pzbv81u.canarytokens.com
st7hjpmcos3hz2xi5pzbv81u.canarytokens.com has address 52.18.63.80
host:~ attacker$
Canarytoken triggered

A DNS Canarytoken has been triggered by the Source IP 34.242.239.31. Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

<table>
<thead>
<tr>
<th>Channel</th>
<th>DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>2019-08-14 01:49:57</td>
</tr>
<tr>
<td>Canarytoken</td>
<td>st7hpnmcos3hz2xi5pzvb8lu</td>
</tr>
<tr>
<td>Token Reminder</td>
<td>USENIX Demo - DNS</td>
</tr>
<tr>
<td>Token Type</td>
<td>dns</td>
</tr>
<tr>
<td>Source IP</td>
<td>34.242.239.31</td>
</tr>
</tbody>
</table>

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)
# cooler

Feb 1st

02:05

mls

waves

Posted using /giphy (2 MB)
Hey Everyone! Here is a link to the TOPSECRETPASSWORDVAULT:
http://canarytokens.com/articles/feedback/jgrufu7my71fwm9bgf5y3k/contact.php
Canarytokens by Thinkst

What is this and why should I care?

Select your token

- Web bug / URL token
  Alert when a URL is visited
- DNS token
  Alert when a hostname is requested
- Unique email address
  Alert when an email is sent to a unique address
- Custom Image Web bug
  Alert when an image you uploaded is viewed
- Microsoft Word Document
  Get alerted when a document is opened in Microsoft Word
- Acrobat Reader PDF Document
  Get alerted when a PDF document is opened in Acrobat Reader
- Windows Folder
  Be notified when a Windows Folder is browsed in Windows Explorer
- Custom exe / binary
  Fire an alert when an EXE or DLL is executed
- Cloned Website
  Trigger an alert when your website is cloned
- SQL Server
  Get alerted when MS SQL Server databases are accessed
- QR Code
  Generate a QR code for physical tokens
- ChiN
<table>
<thead>
<tr>
<th>Token Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web bug / URL token</td>
<td>Alert when a URL is visited</td>
</tr>
<tr>
<td>DNS token</td>
<td>Alert when a hostname is requested</td>
</tr>
<tr>
<td>Unique email address</td>
<td>Alert when an email is sent to a unique address</td>
</tr>
<tr>
<td>Custom Image Web bug</td>
<td>Alert when an image you uploaded is viewed</td>
</tr>
<tr>
<td>Microsoft Word Document</td>
<td>Get alerted when a document is opened in Microsoft Word</td>
</tr>
<tr>
<td>Acrobat Reader PDF Document</td>
<td>Get alerted when a PDF document is opened in Acrobat Reader</td>
</tr>
<tr>
<td>Windows Folder</td>
<td>Be notified when a Windows Folder is browsed in Windows Explorer</td>
</tr>
<tr>
<td>Custom exe / binary</td>
<td>Fire an alert when an EXE or DLL is executed</td>
</tr>
<tr>
<td>Cloned Website</td>
<td>Trigger an alert when your website is cloned</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Get alerted when MS SQL Server databases are accessed</td>
</tr>
<tr>
<td>QR Code</td>
<td>Generate a QR code for physical tokens</td>
</tr>
<tr>
<td>SVN</td>
<td>Alert when someone checks out an SVN repository</td>
</tr>
<tr>
<td>AWS keys</td>
<td>Alert when AWS key is used</td>
</tr>
<tr>
<td>Fast Redirect</td>
<td>Alert when a URL is visited, User is redirected</td>
</tr>
<tr>
<td>Slow Redirect</td>
<td>Alert when a URL is visited, User is redirected, Moar info is grabbed!</td>
</tr>
</tbody>
</table>
Your MS Word token is active!

Download your MS Word file

You'll get an alert whenever this document is opened in Microsoft Office, on Windows or Mac OS.

You can rename the document without affecting its operation.

Ideas for use:

- Drop the file on a Windows network share.
- Leave the file on a web server in an inaccessible directory, to detect webserver breaches.
- Attach to an email with a tempting Subject line.

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.

Canarytoken triggered

An HTTP Canarytoken has been triggered by the Source IP 34.242.239.31.

Basic Details:

<table>
<thead>
<tr>
<th>Channel</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>2019-08-14 03:24:05</td>
</tr>
<tr>
<td>Canarytoken</td>
<td>x3gn14dowo1598emuxs3sdwx9</td>
</tr>
<tr>
<td>Token Reminder</td>
<td>USENIX Demo - Desktop</td>
</tr>
<tr>
<td>Token Type</td>
<td>ms_word</td>
</tr>
<tr>
<td>Source IP</td>
<td>34.242.239.31</td>
</tr>
<tr>
<td>User Agent</td>
<td>Mozilla/4.0 (compatible; ms-office; MSOffice 16)</td>
</tr>
</tbody>
</table>

Canarytoken Management Details:

- Manage this Canarytoken [here](#)
- More info on this token [here](#)

Powered by: Thinkst Canary
In October of 2016 I created a word doc from canarytoken.org and called it
.doc and hid it on the server, outside of IIS. So you would either have to
logon to the box or escape IIS to find the
doc.
In December, we decommissioned the box, took it off line and destroyed it. Starting on
Jan 08 through Jan 17 we have received notification that
the token has been opened five times from
the russian based

We would have no idea that was going on...none.

Thanks,
Create your Canarytoken

Token:
MS Word (Macro)

Reminder:
Document placed in private folder

Close  Create new Canarytoken
Canarytoken triggered (MS Word Macro-enabled: On my laptop)

Canary Name: Canarytokens
Description: Canarytoken triggered
Memo: On my laptop
Token: Macroed MS Word Doc opened
Source IP: 198.235.211.133

More Details
Date: Wed Aug 14 2019 03:48:20 GMT+0000 (UTC)
Login Username: bradley
IP Address: 192.168.2.50
Operating System: Mac OSx
Source IP: 198.235.211.133 (refers to DNS Server and not host)
Select your token

- **Web bug / URL token**
  Alert when a URL is visited

- **DNS token**
  Alert when a hostname is requested

- **Unique email address**
  Alert when an email is sent to a unique address

- **Custom Image Web bug**
  Alert when an image you uploaded is viewed

- **Microsoft Word Document**
  Get alerted when a document is opened in Microsoft Word

- **Acrobat Reader PDF Document**
  Get alerted when a PDF document is opened in Acrobat Reader

- **Windows Folder**
  Be notified when a Windows Folder is browsed in Windows Explorer

- **Custom exe / binary**
  Fire an alert when an EXE or DLL is executed

- **Cloned Website**
  Trigger an alert when your website is cloned

- **SQL Server**
  Get alerted when MS SQL Server databases are accessed

- **QR Code**
  Generate a QR code for physical tokens

- **SVN**
  Alert when someone checks out an SVN repository

- **AWS keys**
  Alert when AWS key is used

- **Fast Redirect**
  Alert when a URL is visited, User is redirected

- **Slow Redirect**
  Alert when a URL is visited, User is redirected (Moar info is grabbed!)
<table>
<thead>
<tr>
<th>Select your token</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web bug / URL token</strong></td>
</tr>
<tr>
<td>Alert when a URL is visited</td>
</tr>
<tr>
<td><strong>DNS token</strong></td>
</tr>
<tr>
<td>Alert when a hostname is requested</td>
</tr>
<tr>
<td><strong>Unique email address</strong></td>
</tr>
<tr>
<td>Alert when an email is sent to a unique address</td>
</tr>
<tr>
<td><strong>Custom Image Web bug</strong></td>
</tr>
<tr>
<td>Alert when an image you uploaded is viewed</td>
</tr>
<tr>
<td><strong>Microsoft Word Document</strong></td>
</tr>
<tr>
<td>Get alerted when a document is opened in Microsoft Word</td>
</tr>
<tr>
<td><strong>Acrobat Reader PDF Document</strong></td>
</tr>
<tr>
<td>Get alerted when a PDF document is opened in Acrobat Reader</td>
</tr>
<tr>
<td><strong>Windows Folder</strong></td>
</tr>
<tr>
<td>Be notified when a Windows Folder is browsed in Windows Explorer</td>
</tr>
<tr>
<td><strong>Custom exe / binary</strong></td>
</tr>
<tr>
<td>Fire an alert when an EXE or DLL is executed</td>
</tr>
<tr>
<td><strong>Cloned Website</strong></td>
</tr>
<tr>
<td>Trigger an alert when your website is cloned</td>
</tr>
<tr>
<td><strong>SQL Server</strong></td>
</tr>
<tr>
<td>Get alerted when MS SQL Server databases are accessed</td>
</tr>
<tr>
<td><strong>QR Code</strong></td>
</tr>
<tr>
<td>Generate a QR code for physical tokens</td>
</tr>
<tr>
<td><strong>SVN</strong></td>
</tr>
<tr>
<td>Alert when someone checks out an SVN repository</td>
</tr>
<tr>
<td><strong>AWS keys</strong></td>
</tr>
<tr>
<td>Alert when AWS key is used</td>
</tr>
</tbody>
</table>

**AWS keys**
Alert when AWS key is used
Canarytokens by Thinkst

What is this and why should I care?

AWS keys

haroon@thinkst.com

USENIX Demo - CEO's Laptop

Create my Canarytoken

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. Know. When it matters.

Your AWS key token is active!

Copy this credential pair to your clipboard to use as desired:

```
[default]
aws_access_key_id = AKIAJ5OM5X2GDP9M4UHIGI
aws_secret_access_key = 8dyW2ZD1wBppbFLAreqs5QHiq2qKhons1j6w
output = json
region = us-east-2
```

Download your AWS Creds

This canarytoken is triggered when someone uses this credential pair to access AWS programmatically (through the API).

The key is hyper unique. i.e. There is 0 chance of somebody having guessed these credentials.

If this token fires, it is a clear indication that this set of keys has "leaked".

Ideas for use:

- These credentials are often stored in a file called ~/.aws/credentials on linux/OSX systems. Generate a fake credential pair for your senior developers
Canarytokens Server

AWS Services

Requests AWS API key

API Gateway

Lambda

Create User with 0 privileges

Generate API key

Respond with AWS API key
Detecting Reverse Engineering with Canaries

Collin Mulliner
Security Researcher and Engineer

collin@3blabs.com
Twitter: @collinrm

Taking the Canary Out of the Coal Mine

Intrusion Detection at Scale

Mike Ruth, Staff Security Engineer
@Cruise Automation
The concept and use of canary tokens has made me very hesitant to use credentials gained during an engagement, versus finding alternative means to an end goal. If the aim is to increase the time taken for attackers, canary tokens work well.
the world is too fluid
So... Don’t buy anything?
The UNIX Philosophy

1. Make each program do one thing well. To do a new job, build afresh rather than complicate old programs by adding new "features".

2. Expect the output of every program to become the input to another, as yet unknown, program. Don't clutter output with extraneous information. Avoid stringently columnar or binary input formats. Don't insist on interactive input.

3. Design and build software, even operating systems, to be tried early, ideally within weeks. Don't hesitate to throw away the clumsy parts and rebuild them.

4. Use tools in preference to unskilled help to lighten a programming task, even if you have to detour to build the tools and expect to throw some of them out after you've finished using them.

https://archive.org/details/bstj57-6-1899
Perfect is the enemy of Good
Know Your Enemy: Sebek

A kernel based data capture tool

The Honeynet Project
http://www.honeynet.org
Last Modified: 17 November 2003

Introduction:

Back at Berkley in the 1980's, Cliff Stoll quickly ran into a problem that still vexes honeynet researchers today: How do you observe an intruder without them noticing? In Cliff's situation he was able to directly monitor serial lines to capture the keystrokes of the intruder. Much has changed since then, however, our fundamental challenge has remained the same: How can we capture the activities of an intruder without them knowing? It is critical that a honeynet designed for the purposes of observing human intruders looks and behaves as any normal system, thus we must ensure that the intruder cannot detect that he or she is being observed. The traditional approach is to capture these activities by recording the associated network data. This is a desirable approach because it can be done in such a way as to be invisible to the intruder.

To nobody's surprise, Blackhat hackers haven't stood still. It is increasingly common for even the most basic intruders to utilize encryption to protect their communications channels. If encryption services are not available on the victim host, it is not uncommon for them to install their own trusted services such as SSH, an encrypted GUI client, or SSL. Without the key, network based data capture tools are unable to view this channel.

To observe intruders using session encryption, researchers needed to find a way to break the session encryption. For many organizations this has proven extremely difficult. In an attempt to circumvent session encryption rather than break it, the HoneyNet Project began experimenting with using kernel-based toolskits for the purpose of capturing the data of interest from within the honeypot's kernel. These experiments lead to the development of a tool called Sebek. This tool is a piece of code the lives entirely in kernel space and records either some or all data accessed by users on the system. It provides capabilities to recent keystrokes of a session that is using encryption, recover files with SCP, capture passwords used to log in to remote systems, recover passwords used to enable BURNEY protected chniches and accompany many other forensics related tasks. This paper discusses Sebek version 2 which will be referred to as Sebek.

What follows is a detailed discussion of Sebek, how it works and its value. We will examine the architecture and key components. From there, we will drill down into the implementation issues and technical details of operation. Finally, we will show a usage example demonstrating the use of Sebek including its new web interface.

The Sebek development cycle starts on a Linux system. Sebek is ported to other Operating Systems such as Win32, Solaris, and OpenBSD after it working on Linux. As a result, this paper, and its examples, will be based on the Linux version of Sebek, however many of the concepts discussed here apply to the other ports as well.

---

We don’t have to be perfect
We don’t have to win every battle
If it’s stupid, but works...

Then its not stupid
Build Products
But we aren’t [Google|Slack|Square...]
“Embrace the Hack”