COOKIE CADGER

Matthew Sullivan @MattsLifeBytes | MattsLifeBytes.com

Things I've Learned At Derbycon

- Dinner here is expensive
  - $460,000 at the Maker's Mark Lounge
- Don't try to play with hotel display systems
  - No, we didn't get caught…
  - But we left terrified of how the highest-end hotels in downtown Louisville store their guests' data

Obligatory "Who Am I" Slide Here

- Graduate student
  - Iowa State University
  - Information Assurance + Computer Engineering
    - Graduating in May, 2013
  - Research Assistant
    - Internet-Scale Attack and Event Generation Environment (ISEAGE)
- In my free time
  - I like to make stuff
  - And break stuff

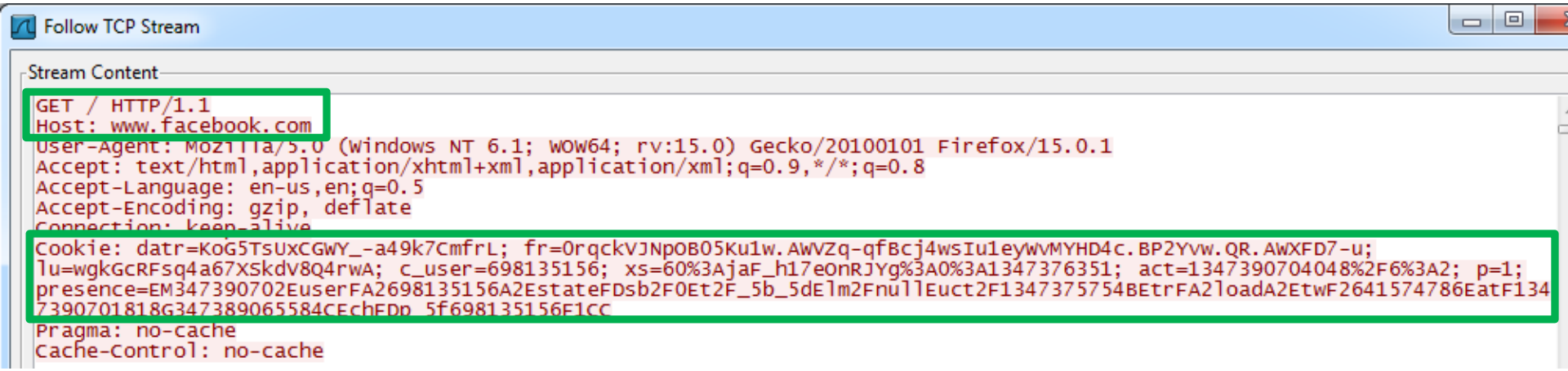
What The Heck is a Cookie?

Cookies in 30 Seconds

1. Click a link
2. Browser sends information to a web server
   - Sends a request asking for a specific page
   - Includes some hidden information, including cookie data
3. The web server figures out your identity based on your cookie data
4. Web server returns the page you requested, tailored just for you

How The Internet Works

- Example, using Facebook
- I am logged in and I visit the home page



- Web server matches this cookie information
- Lets me view a page customized just for me!

facebook

Search for people, places and things

Matthew Sullivan | Home

Matthew Sullivan

FAVORITES

- News Feed
- Messages 2
- Events 1

ADS

- Ads Manager

PAGES

- Information Assurance Stud...

GROUPS

- ISEAGE and Friends
- ISU Computer Majors
- IASG
- Add Group...

APPS

- App Center 1
- Photos
- Twitter
- Games Feed 20+
- Music

MORE

Update Status | Add Photo / Video | Ask Question

What's on your mind?

SORT

Robert Anhalt

"Is the server down?"
Yep. We only have one server. It does everything. And it's down.

Like · Comment · 17 minutes ago ·

Write a comment...

Leah Hallgren

Thoughts, prayers and ♥ to Kari Beth Hamilton & Joy Eschenbrenner Latcham as they remember their mom today. She was definitely a postive and wonderful influence when I was young and treasure the memories I had with their family at that time. ♥

Like · Comment · Share · 13 minutes ago near East Ottumwa, IA ·

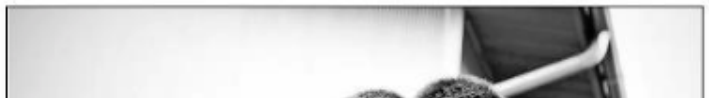
Matthew Lorimor

http://distilleryimage7.instagram.com/26ea7382fb7e11e18c8422000a1cbdd4_7.jpg

http://distilleryimage7.instagram.com/26ea7382fb7e11e18c8422000a1cbdd4_7.jpg
distilleryimage7.instagram.com

Like · Comment · Share · about an hour ago ·

JJ Grinvalds changed his profile picture.



Create Event

1 Bejeweled Blitz request

Sponsored | Create an Ad

Barack Obama
If you're fired up right now, if you've got Barack Obama's back, then own a piece of this ...

Like This Page

Nate Evans likes TriPom Chews.

TriPom Chews
Like

Alyssa J Louwsma, Tyler Orman, and Emily Orman like Beef. It's What's For Dinner.

Beef. It's What's For Dinner.
Like

Keith J Abel likes AmesTornadoWash.

AmesTornadoWash
Like

Character Counts In Iowa
Miracles start to happen when you give as much energy to your dreams as you do your fears. -Unknown

Firesheep: OMGZ NEW SPLOITZ

- For the uninitiated:
  - Firesheep was rather… unstable
  - Not maintained and hasn't worked since Firefox 3.x
  - Made to scare large entities like Facebook, Twitter
    - And companies
    - And people
  - Was never meant to be more than a:
    "hey guys, this is a really big problem"

Firesheep: OMGZ NEW SPLOITZ

- The world was like
  - HOLY CRAP
- And businesses everywhere were like
  - HOLY CRAP
- And InfoSec was like
  - Yeah… duh
- And Facebook was like
  - Naw… it's *fine*

So I had this piece of crap

- Called “ISESpy”
- Which watched for HTTP GET requests
- And then re-opened them in Firefox
- It was terri-bad

So I had this piece of crap

- Very effective tool
- Especially at Iowa State
  - Brace yourselves… it's pretty bad
- All wireless is "IASTATE"
  - No keys required. There's not even an additional SSID with the option for it.

And then I had a class project

- Make a cool project
- That has something to do with wireless
- Pretty much no other requirements
- YAY!

Thus, Cookie Cadger Was Born

- **cadge**

  verb, **cadged, cadg·ing**

  to beg or obtain by begging.

Cookie Cadger

- A pen testing tool, not just a toy
  - Detailed HTTP request capturing
  - Replay of lots of things:
    - Requested item
    - User agent
    - Referer
    - Basic authorization
- In short: find request » replay request » win

Cookie Cadger

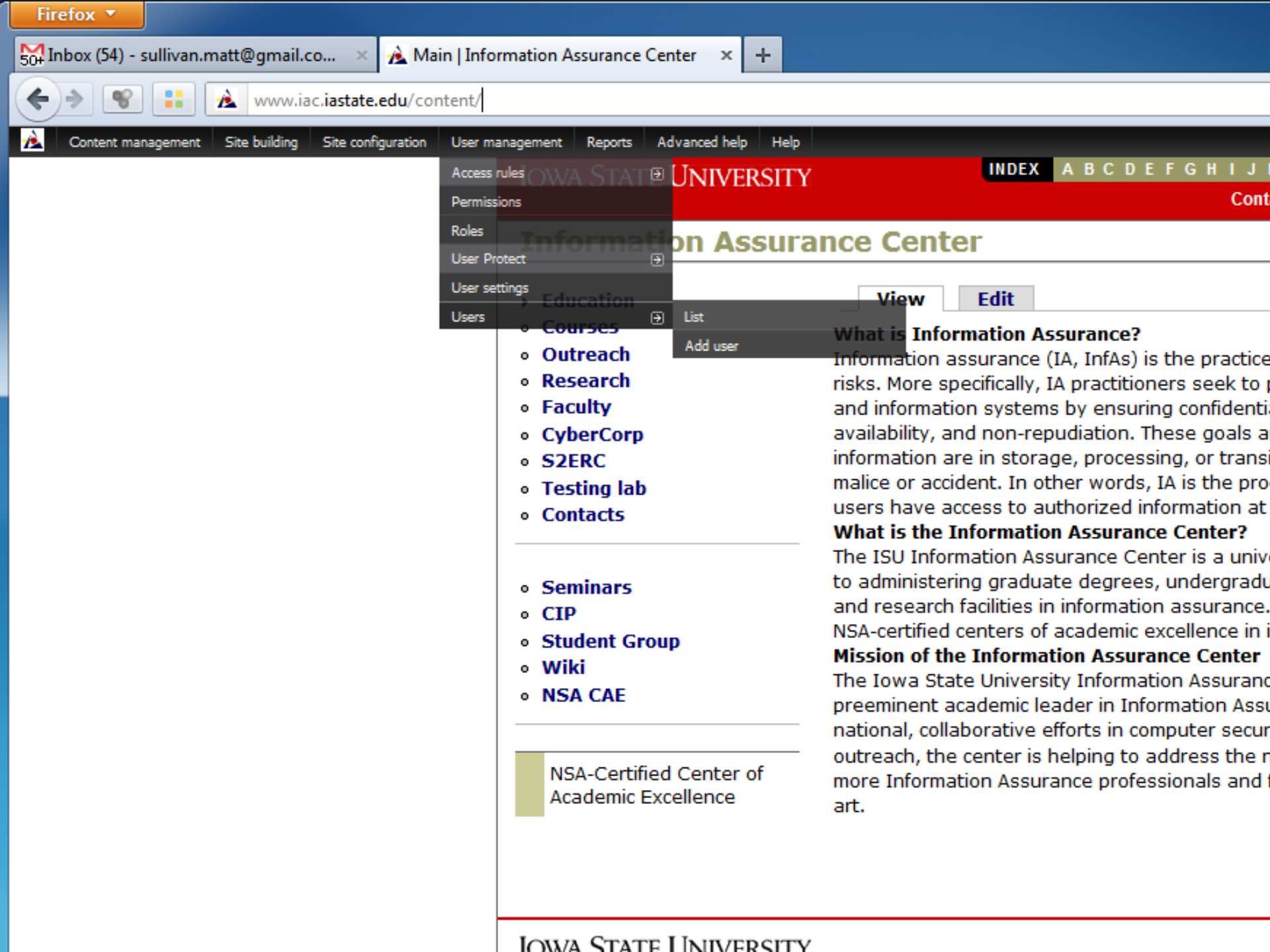
- Live analysis
  - Wi-Fi
  - Wired
- pcap file analysis
  - Lots of fun ways to get those
  - Mobile exploitation and analysis

Cookie Cadger

- Dataset handling
  - Save current
  - Load previous
- Dataset features
  - Sqlite3
- A decent schema
  - Which opens up the door to other cool things

Cookie Cadger

- Session detection
  - Anyone can write their own plugins in JavaScript
  - Drop it into the plugins directory
- Some already provided for you
  - Facebook
  - Twitter
  - Reddit
  - Drupal
  - phpBB3
  - Wordpress


Firefox
Inbox (54) - sullivan.matt@gmail.co...
Main | Information Assurance Center
www.iac.iastate.edu/content/
Content management
Site building
Site configuration
User management
Reports
Advanced help
Help
Access rules
Permissions
Roles
User Protect
User settings
Users
List
Add user
INDEX
A B C D E F G H I J
Cont
Assurance Center
View
Edit
Education
Courses
Outreach
Research
Faculty
CyberCorp
S2ERC
Testing lab
Contacts
Seminars
CIP
Student Group
Wiki
NSA CAE
NSA-Certified Center of Academic Excellence
What is Information Assurance?
What is the Information Assurance Center?
Mission of the Information Assurance Center
art.

Cookie Cadger

- Obvious use-cases:
  - Pwn someone and prove that open Wi-Fi is not a good idea
- Great for checking for leaky applications
  - My own website!

Cookie Cadger

Time to pray to the demo gods!

Cookie Cadger

- Binary available now
  - We're helping Hackers for Charity!

    https://CookieCadger.com

- Source available in the middle of October
  - Because I am horrible at Java
  - FreeBSD license

- Not going to be abandonware
  - At least until after May…

Credits

- Travel and support for the project
  - Iowa State University's Information Assurance Center

    https://www.iac.iastate.edu

- Help with everything else

https://CookieCadger.com

[Every download helps HFC!]

Tweet with #CookieCadger if you have questions, comments, suggestions. I'll try to keep an eye on it!

Matthew Sullivan @MattsLifeBytes | MattsLifeBytes.com