Administrative

- Guest Lecture Today
    - Windows
    - Protection
- Course Evaluations

Linux and Windows

- We have talked about Linux a lot in this class, but what about Microsoft Windows?

Modifying the Windows Kernel

- Everything is done via drivers
  - Which look a little like Loadable Kernel Modules in Linux
- Resources:
  - Hardware
    - Graphics cards
    - Network cards
  - Software
    - File system
    - Network stack

A Taste of Windows Kernel

- Created a start-up company
- Kernel driver for network flows
  - Plus, a Windows service to get user-side data
- Libraries available:
  - Windows Filtering Platform (WFP)
  - Network Sockets (WSK)
  - Cryptography (CNG)
  - Debug Console

Debugging Windows

- Gentle suggestions about bugs
  - Commonly called “Blue Screens of Death”
- Debugging typically done “off host”
  - Via serial connection
  - Via Ethernet
  - Via shared memory (VirtualKD)
- WinDbg somewhat like gdb/ddd
- DbgPrint somewhat like printk in Linux

An Interesting Wrinkle

- What are IRQs?
- What happens when you turn “interrupts off”?
- Windows has IRQ levels:

IRQL	X86 IRQL Value	AMD64 IRQL Value	IA64 IRQL Value	Description
PASSIVE_LEVEL	0	0	0	User threads and most kernel-mode operations
APC_LEVEL	1	1	1	Asynchronous procedure calls and page faults
DISPATCH_LEVEL	2	2	2	Thread scheduler and deferred procedure calls (DPCs)
CMC_LEVEL	N/A	N/A	3	Correctable machine-check level (IA64 platforms only)
Device interrupt levels (DIRQL)	3-26	3-11	4-11	Device interrupts
PC_LEVEL	N/A	N/A	12	Performance counter (IA64 platforms only)
PROFILE_LEVEL	27	15	15	Profiling timer for releases earlier than Windows 2000
SYNCH_LEVEL	27	13	13	Synchronization of code and instruction streams across processors

Managing IRQ Levels

- Locks and Synchronization
- Function calls have maximum IRQ levels

Windows Kernel

- Would more on this be interesting to you?

OS Protection

Systems Security

- Stories
- Relevant Research Projects
- MQPs
  - Check your email; you have spam!
- Jobs/Internships?
- Scholarship for Service Program
  - Applications due at 11:59:59.999pm tomorrow

Cyber Security and Game Theory

- Active opponents
  - Cat and mouse game

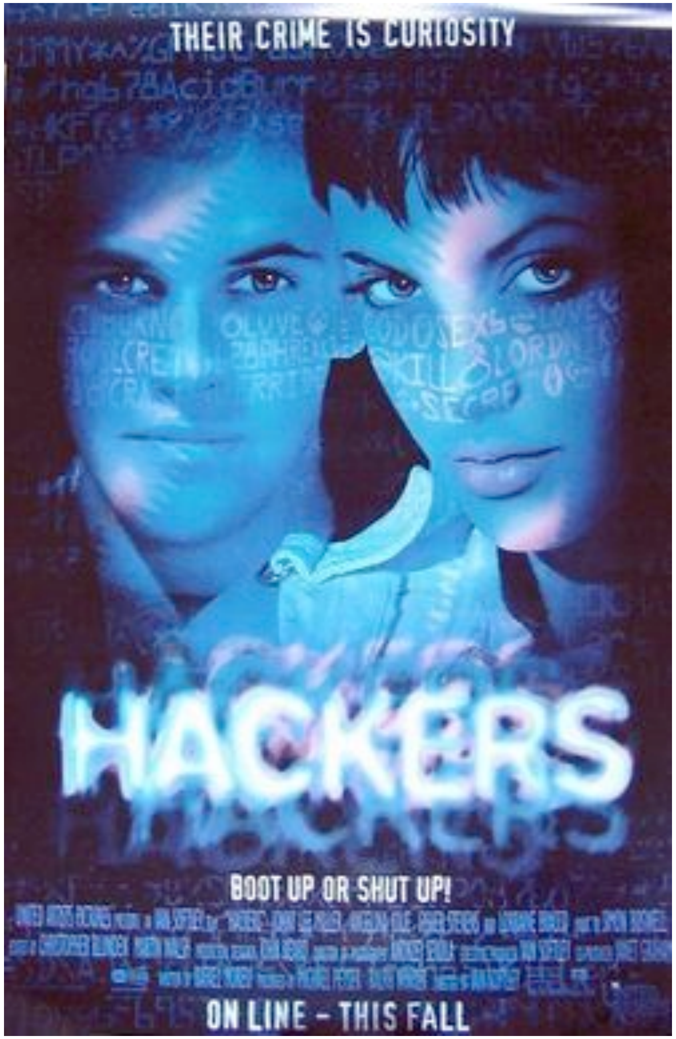
- It’s not whether you root or not, it’s how you exploit the system
  - No preying on newbies

- What do attackers call “Winning Dirty”?

Adversaries

- Intruders/Attackers
- Divine intervention
- System errors
- Human error

- A word on insider threats



Insider Attacks

- Logic bombs
- Trap doors
  - Code reviews
- Login spoofers
  - Why ctrl+alt+delete?

Focus: Insider Threat

Insider Threat

- Malicious actors within an organization
- Motivations
  - Competitive Advantage
  - Financial Gain
- Of surveyed organizations in 2007
  - 49% had at least one deliberate insider incident within last year
  - One organization lost $100 million as a result

Some attacks cost more than money

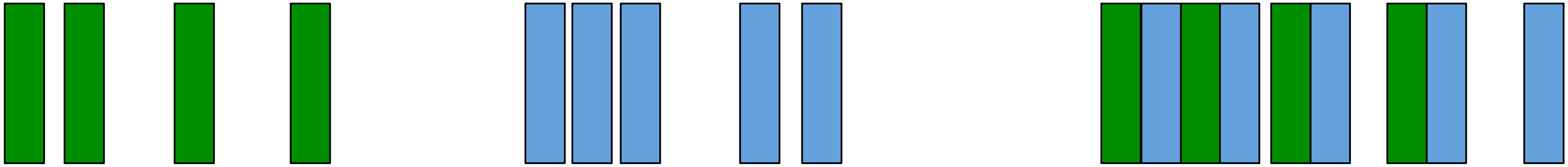
- WikiLeaks exposure of US Department of State diplomatic cables
  - Perpetrated by DoD insider
    - Chelsea Manning
  - Increase foreign tension with US
  - Increased risk to US allies
- Edward Snowden?

An Example: Payroll

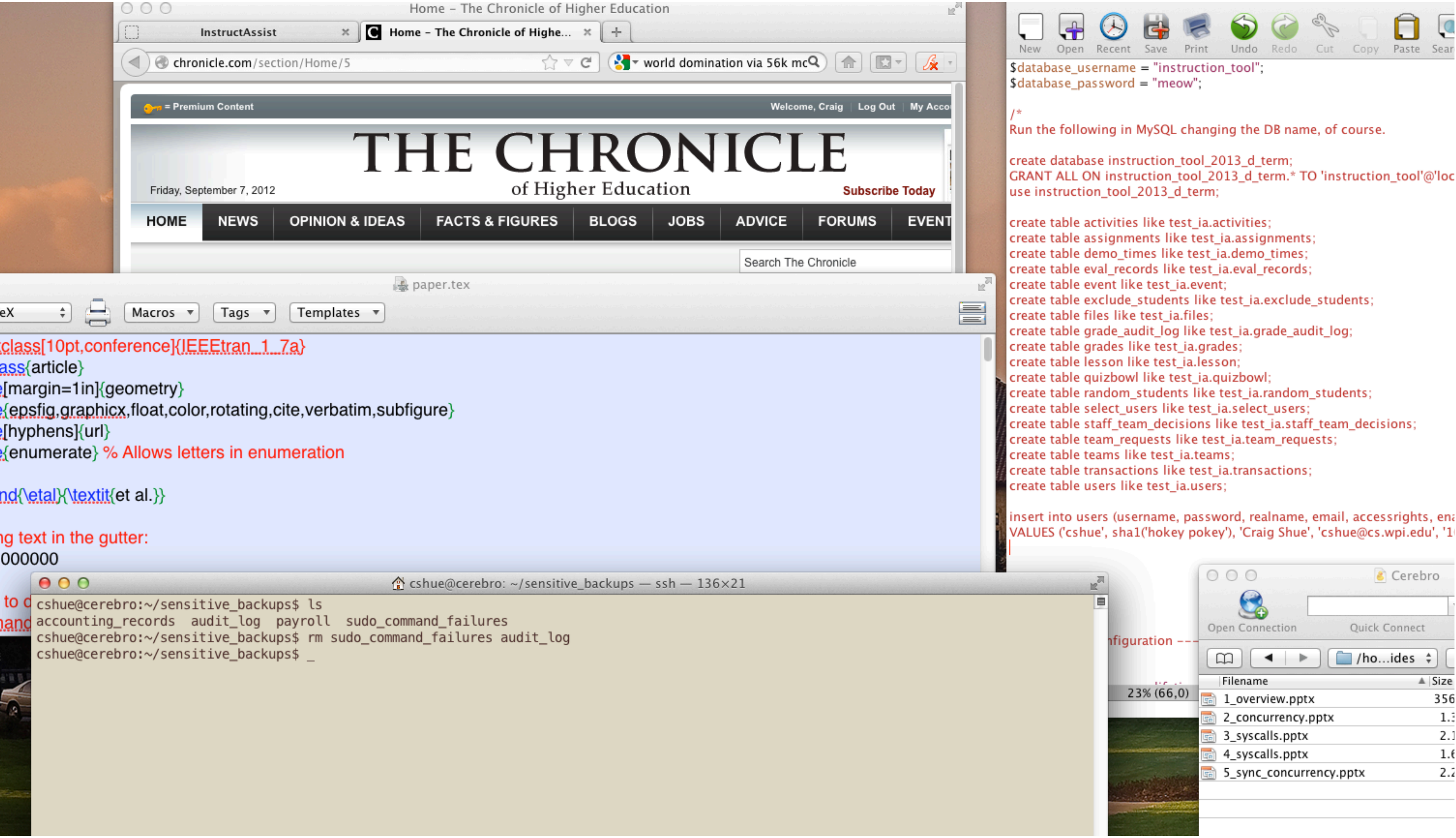
- Payroll manager authorized to manage accounts, transfer funds
- Within own authority, manager could
  - Add a fraudulent payee
  - Pay the payee
  - Delete the payee from the system
- Hard to systematically detect abuse without considering the context

Prior work: A battle with complexity

- System log examination
  - Often too sparse, hard to link actions
- System call behavior
  - Example: all fopen, fread, fclose calls
  - Overwhelming complexity
  - Difficulty of interleaved activities



The Big Picture



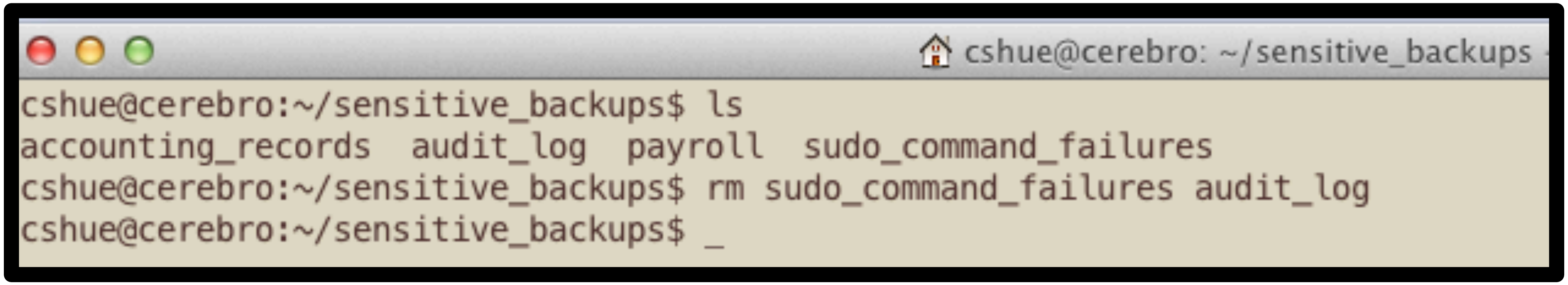
```
class[10pt,conference]{IEEEtran_1_7a}
ass{article}
e[margin=1in]{geometry}
e{epsfig,graphicx,float,color,rotating,cite,verbatim,subfigure}
e[hyphens]{url}
e{enumerate} % Allows letters in enumeration

nd{\etal}{\textit{et al.}}

ng text in the gutter:
000000

 to d
hand
```

```
cshue@cerebro:~/sensitive_backups$ ls
accounting_records  audit_log  payroll  sudo_command_failures
cshue@cerebro:~/sensitive_backups$ rm sudo_command_failures audit_log
cshue@cerebro:~/sensitive_backups$ _
```

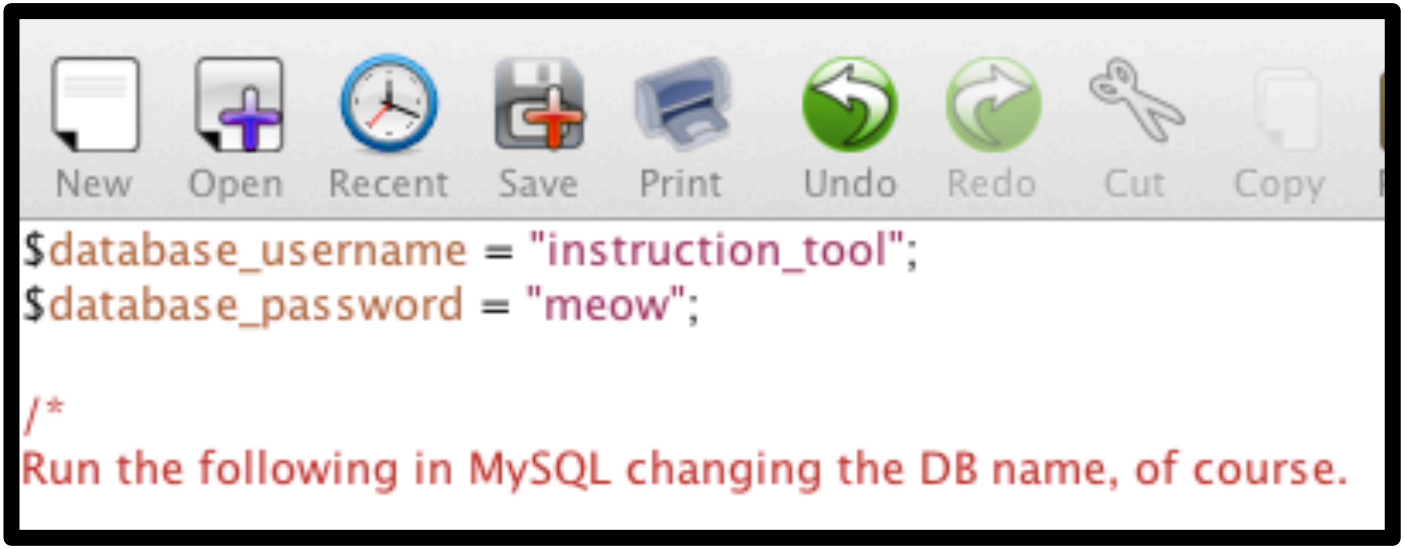
```
$database_username = "instruction_tool";
$database_password = "meow";

/*
Run the following in MySQL changing the DB name, of course.

create database instruction_tool_2013_d_term;
GRANT ALL ON instruction_tool_2013_d_term.* TO 'instruction_tool'@'loc
use instruction_tool_2013_d_term;

create table activities like test_ia.activities;
create table assignments like test_ia.assignments;
create table demo_times like test_ia.demo_times;
create table eval_records like test_ia.eval_records;
create table event like test_ia.event;
create table exclude_students like test_ia.exclude_students;
create table files like test_ia.files;
create table grade_audit_log like test_ia.grade_audit_log;
create table grades like test_ia.grades;
create table lesson like test_ia.lesson;
create table quizbowl like test_ia.quizbowl;
create table random_students like test_ia.random_students;
create table select_users like test_ia.select_users;
create table staff_team_decisions like test_ia.staff_team_decisions;
create table team_requests like test_ia.team_requests;
create table teams like test_ia.teams;
create table transactions like test_ia.transactions;
create table users like test_ia.users;

insert into users (username, password, realname, email, accessrights, ena
VALUES ('cshue', sha1('hokey pokey'), 'Craig Shue', 'cshue@cs.wpi.edu', '1
```

Filename	Size
1_overview.pptx	356
2_concurrency.pptx	1.3
3_syscalls.pptx	2.1
4_syscalls.pptx	1.6
5_sync_concurrency.pptx	2.2

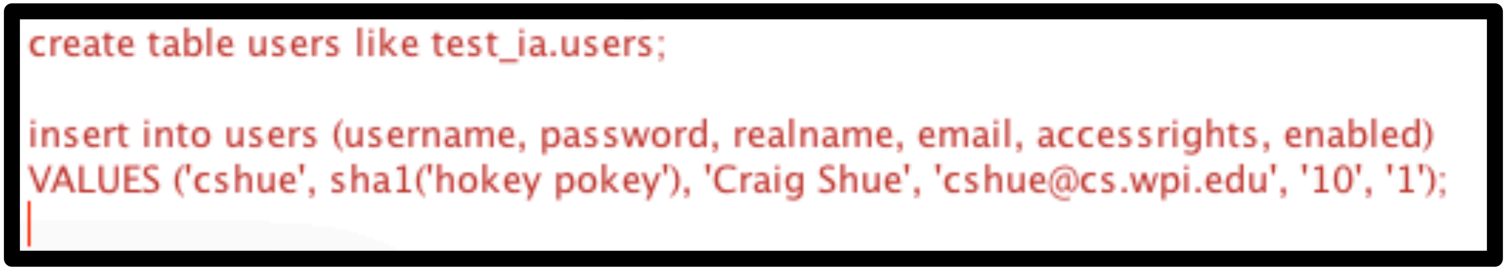
OCR and Keywords



```
cshue@cerebro:~/sensitive_backups$ ls
accounting_records  audit_log  payroll  sudo_command_failures
cshue@cerebro:~/sensitive_backups$ rm sudo_command_failures audit_log
cshue@cerebro:~/sensitive_backups$ _
```

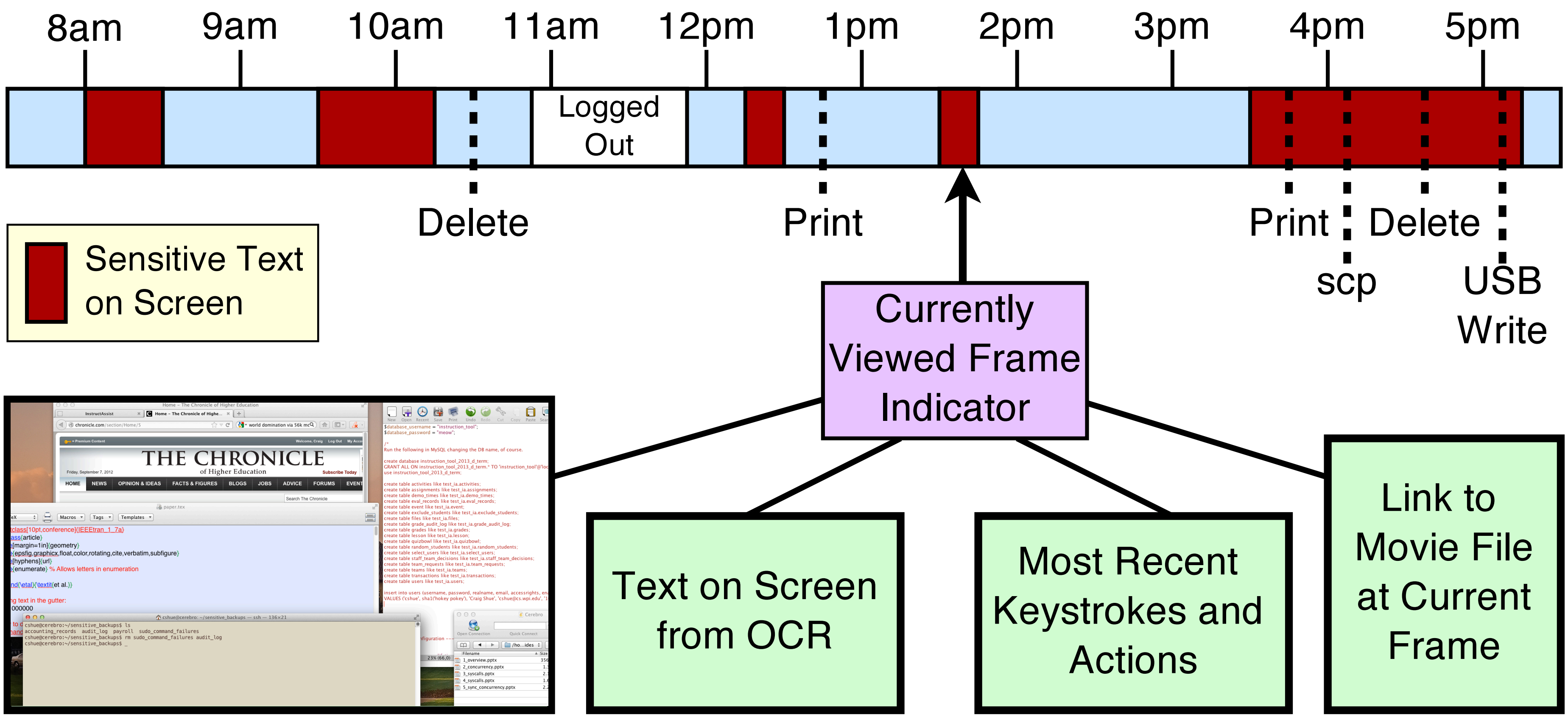


```
$database_username = "instruction_tool";
$database_password = "meow";


/*
Run the following in MySQL changing the DB name, of course.
```



```
create table users like test_ia.users;

insert into users (username, password, realname, email, accessrights, enabled)
VALUES ('cshue', sha1('hokey pokey'), 'Craig Shue', 'cshue@cs.wpi.edu', '10', '1');
```

Auditor Console



```
tclass[10pt,conference]{IEEEtran_1_7a}
ass{article}
e[margin=1in]{geometry}
e{epsfig,graphicx,float,color,rotating,cite,verbatim,subfigure}
e[hyphens]{url}
e{enumerate} % Allows letters in enumeration

nd{\etal}{\textit{et al.}}

ng text in the gutter:
000000
```

```
$database_username = "instruction_tool";
$database_password = "meow";

/*
Run the following in MySQL changing the DB name, of course.

create database instruction_tool_2013_d_term;
GRANT ALL ON instruction_tool_2013_d_term.* TO 'instruction_tool'@'loc
use instruction_tool_2013_d_term;

create table activities like test_ia.activities;
create table assignments like test_ia.assignments;
create table demo_times like test_ia.demo_times;
create table eval_records like test_ia.eval_records;
create table event like test_ia.event;
create table exclude_students like test_ia.exclude_students;
create table files like test_ia.files;
create table grade_audit_log like test_ia.grade_audit_log;
create table grades like test_ia.grades;
create table lesson like test_ia.lesson;
create table quizbowl like test_ia.quizbowl;
create table random_students like test_ia.random_students;
create table select_users like test_ia.select_users;
create table staff_team_decisions like test_ia.staff_team_decisions;
create table team_requests like test_ia.team_requests;
create table teams like test_ia.teams;
create table transactions like test_ia.transactions;
create table users like test_ia.users;

insert into users (username, password, realname, email, accessrights, ena
VALUES ('cshue', sha1('hokey pokey'), 'Craig Shue', 'cshue@cs.wpi.edu', '1
```

cshue@cerebro: ~/sensitive_backups — ssh — 136×21

```
cshue@cerebro:~/sensitive_backups$ ls
accounting_records  audit_log  payroll  sudo_command_failures
cshue@cerebro:~/sensitive_backups$ rm sudo_command_failures audit_log
cshue@cerebro:~/sensitive_backups$ _
```

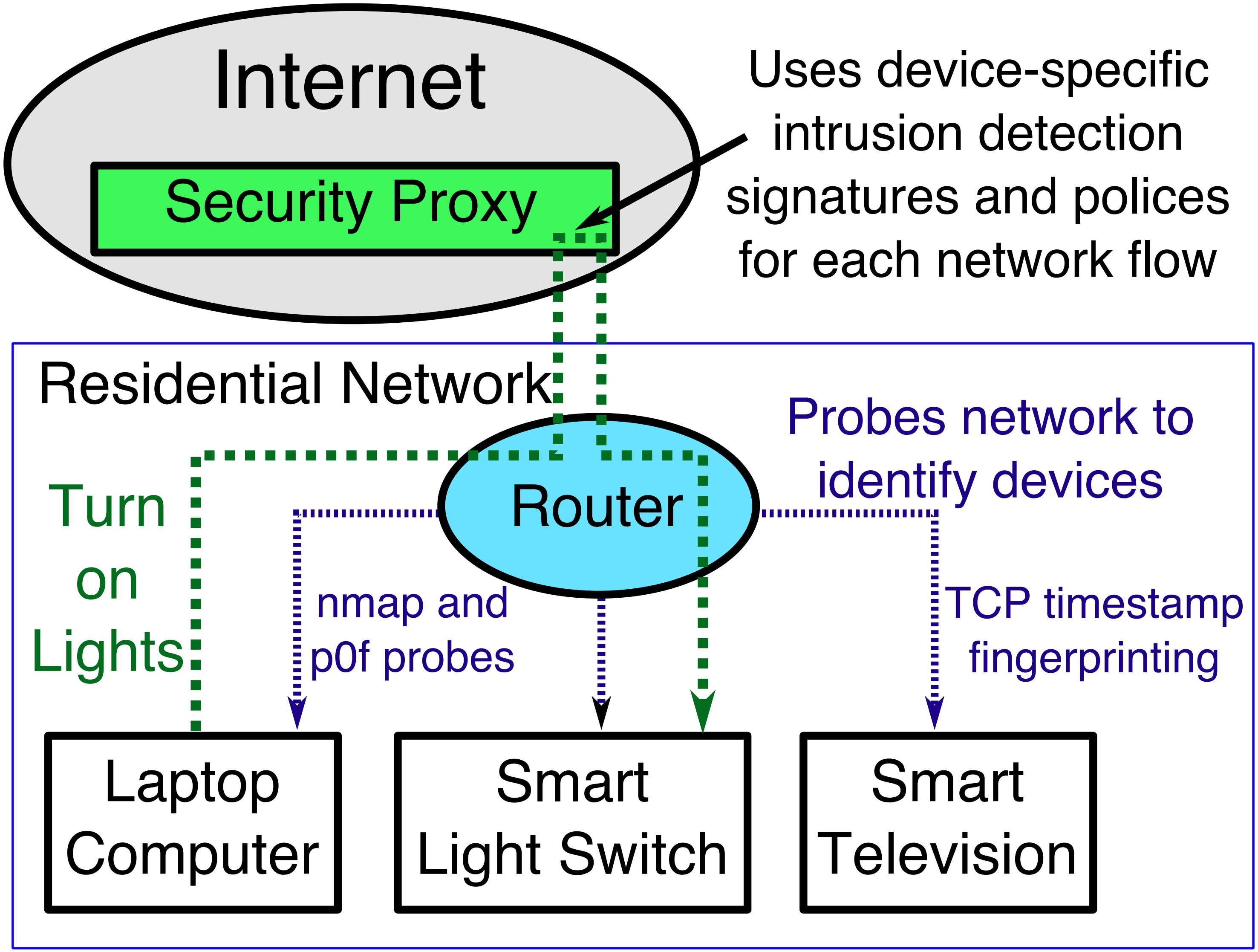
Exploiting Bugs

- Buffer Overflow Attacks
- String format attacks
  - Causing printf to change memory
- Return to libc Attacks
- Integer Overflow Attacks
- Code Injection Attacks
- Privilege Escalation Attacks

Malware

- Backdoor
- Zombies and Botnets
- Keylogger
- Identity Theft
- Viruses, Trojan Horses, Worms
  - Parasitic Viruses
  - Memory Resident
    - Interrupt Vector?
  - Boot Sector

Bringing IT Home: Residential SDN


Internet
Security Proxy
Uses device-specific intrusion detection signatures and polices for each network flow
Residential Network
Probes network to identify devices
Turn on Lights
Router
nmap and p0f probes
TCP timestamp fingerprinting
Laptop Computer
Smart Light Switch
Smart Television

]