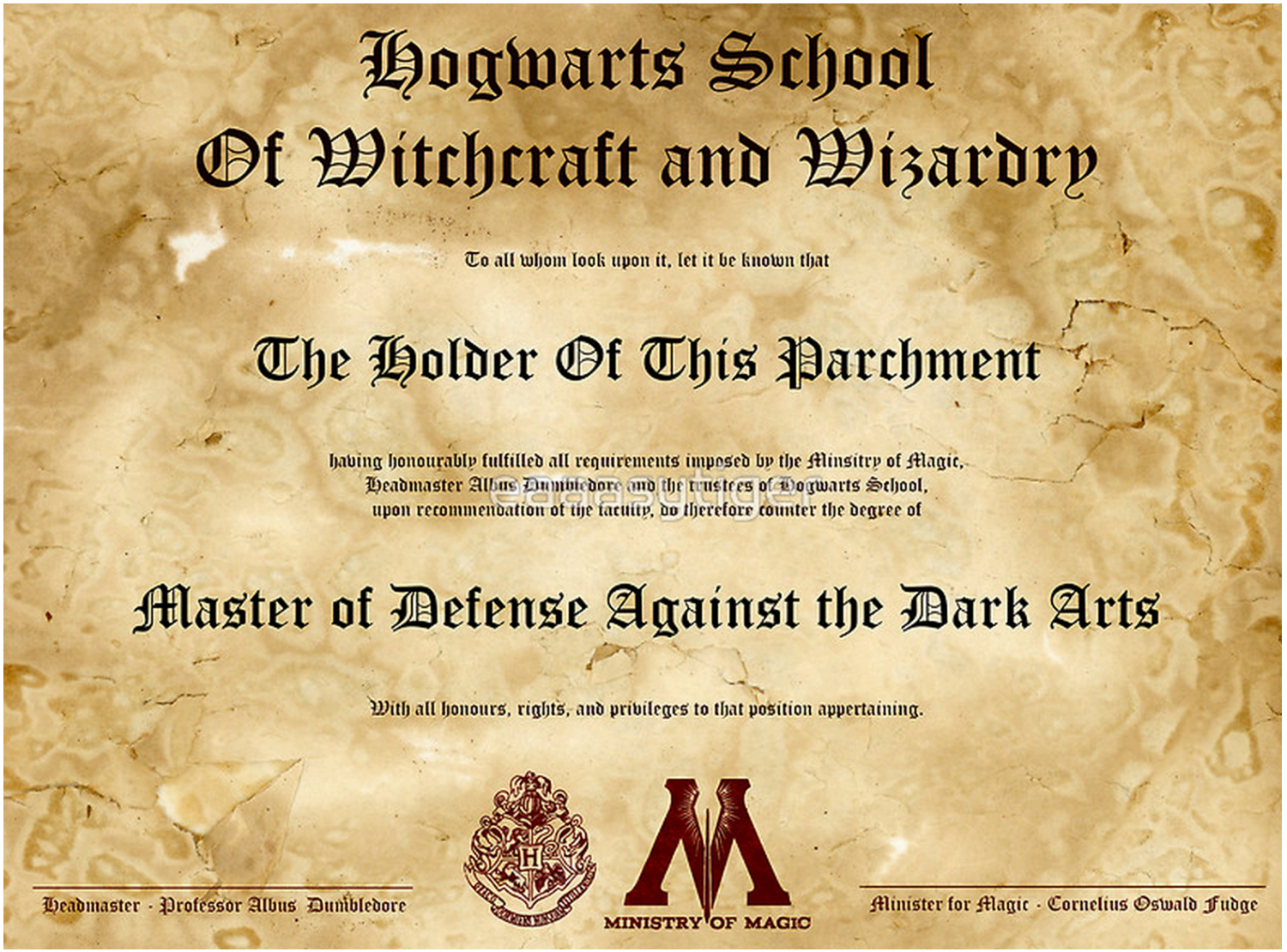
Defending Computer Networks
Lecture 1: Intro

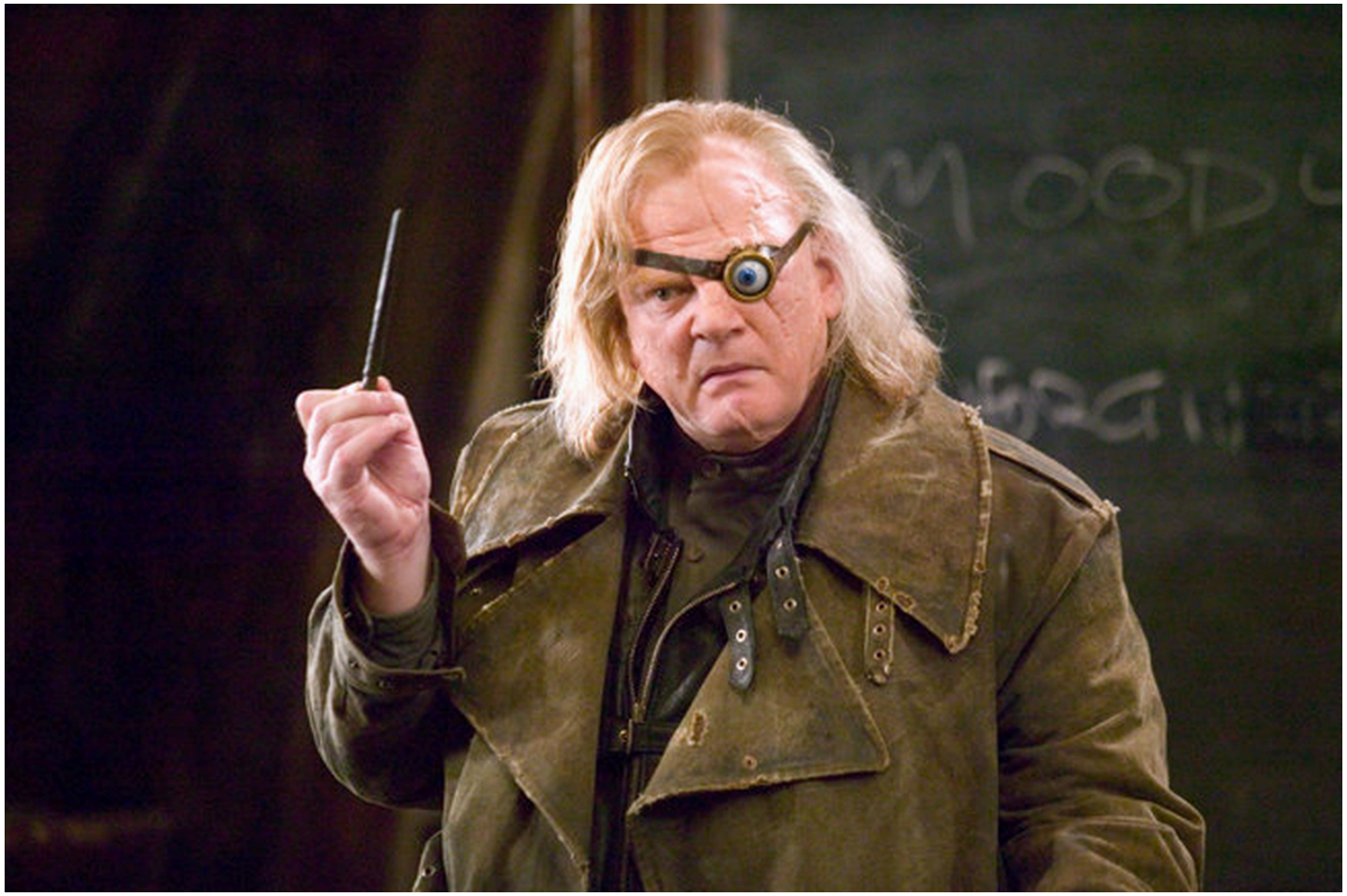
Stuart Staniford
Adjunct Professor of Computer Science
(Also, CEO Cayuga Networks, President Viridius Property,
Ex Chief Scientist FireEye)
Fall 2015

What I Really Wanted to Call The Course



Credit: http://www.redbubble.com/people/eaaasytiger/works/8872016-official-hogwarts-diploma-poster-defense-against-the-dark-arts

Of course, that makes me



Goals For Today

- Class Organization/Logistics
- Motivation: Why this subject matters

Class Description

In this course, we discuss attacks on operational computer networks, with a focus on how to prevent them, or detect them if we fail to prevent them; study the reasons why real-world software tends to be vulnerable, and how attackers exploit those vulnerabilities; talk about the lifecycle of network attacks – methods of reconnaissance, gaining control of bulk volumes of computers via scanning, by worms, or by client-side attacks such as drive-by downloads from malicious websites; discuss the control of the resulting botnets of computers and the motives of attackers such as criminal syndicates and intelligence agencies; cover network-level defenses such as firewalls, encryption and virtual private networks; cover technical approaches for detecting attacks both on the network and on the host; talk about legal and ethical issues for network defenders.

I'll Be Happy If

- You are prepared for a MS grad position
  - With a computer security company.
  - Or an operational network security role on a big network.
- Network Security is a huge field
  - And gets more complex by the year
  - All kinds of detailed sub-specializations
    - Mine is network anomaly detection
  - Cannot hope to do more than gesture at many parts of the field.

Course Size/Status

- Limited to 75
  - By both room and TA resources.
  - M. Eng focussed course,
    - Will open to all with prereqs if space
- Third year of course
  - Prior feedback:
    - Liked course a lot
    - Course is very demanding
    - Learnt a great deal
    - Very valuable in job interviews
  - We are retooling assignment structure this year

Prerequisites

- CS 2022 or equivalent, (C language)
  - You must have learnt C somewhere.
- CS 3410 or equivalent (Architecture),
  - Know what stack, heap, etc are, and have some familiarity with assembly language
- CS 4410 or equivalent (Operating Systems),
  - Need some familiarity with Unix/Linux
- Or consent of instructor.
- Be great if you knew something about networks too.

Website, Office Hrs, etc

- **Class Website:**
  - http://www.cs.cornell.edu/courses/cs5434/2015fa/
- **Instructor Office Hours:**
  - Tuesday: 11:30am-12:30pm.
  - Gates 335.
- **Teaching Assistants.**
  - Zhiyuan Teo (zt27) + one other TBD.
  - Office hours TBD.
- **Piazza/CMS**
  - **Yes, but not set up yet.**

Reading Materials

- There is no textbook for the course.
- My slides will be on web for the lectures.
  - However, these should not be viewed as a substitute for your own note-taking.
- There will be assigned readings of papers, which **comprise part of the course material and which you may be quizzed on**.
- See handout for readings for lectures 1-3.

Evaluation

- 20% in-class quizzes.
  - Dates TBD.
- 10% midterm
- 20% final
- 50% homework assignments.
  - Mostly practical exercises using common network security tools, or coding projects to illustrate principles.

Lateness

- Homeworks/projects turned in late
  - Score reduced by 20% per each day of lateness,
  - or part of a day.
  - After five days down to zero.

Grading Philosophy

- This is MS Eng targeted course.
  - I assume most of you are aiming at industry jobs
  - And I have extensive commercial experience
- So
  - A: would recommend you for any security company
    - at top of pay scale for incoming MS grads
  - B+: solid student, would recommend for any company.
  - B/B-: getting a bit marginal, ok for smaller companies.
  - C: would not recommend.
  - D/F: failing to engage with class.
- Students aiming for academic research in security
  - plan on getting A/A+

Guest Lectures

- Plan to have several guest lectures
  - Towards the end of the course.
- Senior technical security researcher
  - From a security product company.
- Senior operational security person
  - From a big network.
- Goal is to allow you to hear/question people working on this stuff for real every day.
- Their presentations are part of course and will likely be tested on third quiz.

Academic Integrity

- http://cuinfo.cornell.edu/Academic/AIC.html
- In-class quizzes are to be done without consulting anyone or anything other than the student's own memory.
  - Use of phones, tablets, laptops, prepared notes, neighbors, or any other external aid will be considered a violation of academic integrity.
- For lab-based homework assignments,
  - students may consult with each other in general terms,
  - must perform all steps of the assignment themselves, create their own work, and write up their own results.
- For class projects,
  - code should be developed from scratch, using only libraries available on the system.
  - Cut and paste from internet code is not permissible,
  - nor is borrowing of code from other class participants.

Computer Security Ethics

- In this course, you will be learning evil dark arts!
- Computer attack techniques which are
  - **immoral**
  - **illegal**
  - **against university policy**
  - to use in the wild.
- You could get in **very serious trouble**
  - running exploits or network reconnaissance techniques against computers and networks that aren't explicitly sanctioned for educational purposes.
  - No one treats this stuff as a joke any more
- Keep **all attack/recon activity** on computers/networks that you own personally.

Motivation

- Why this stuff matters.

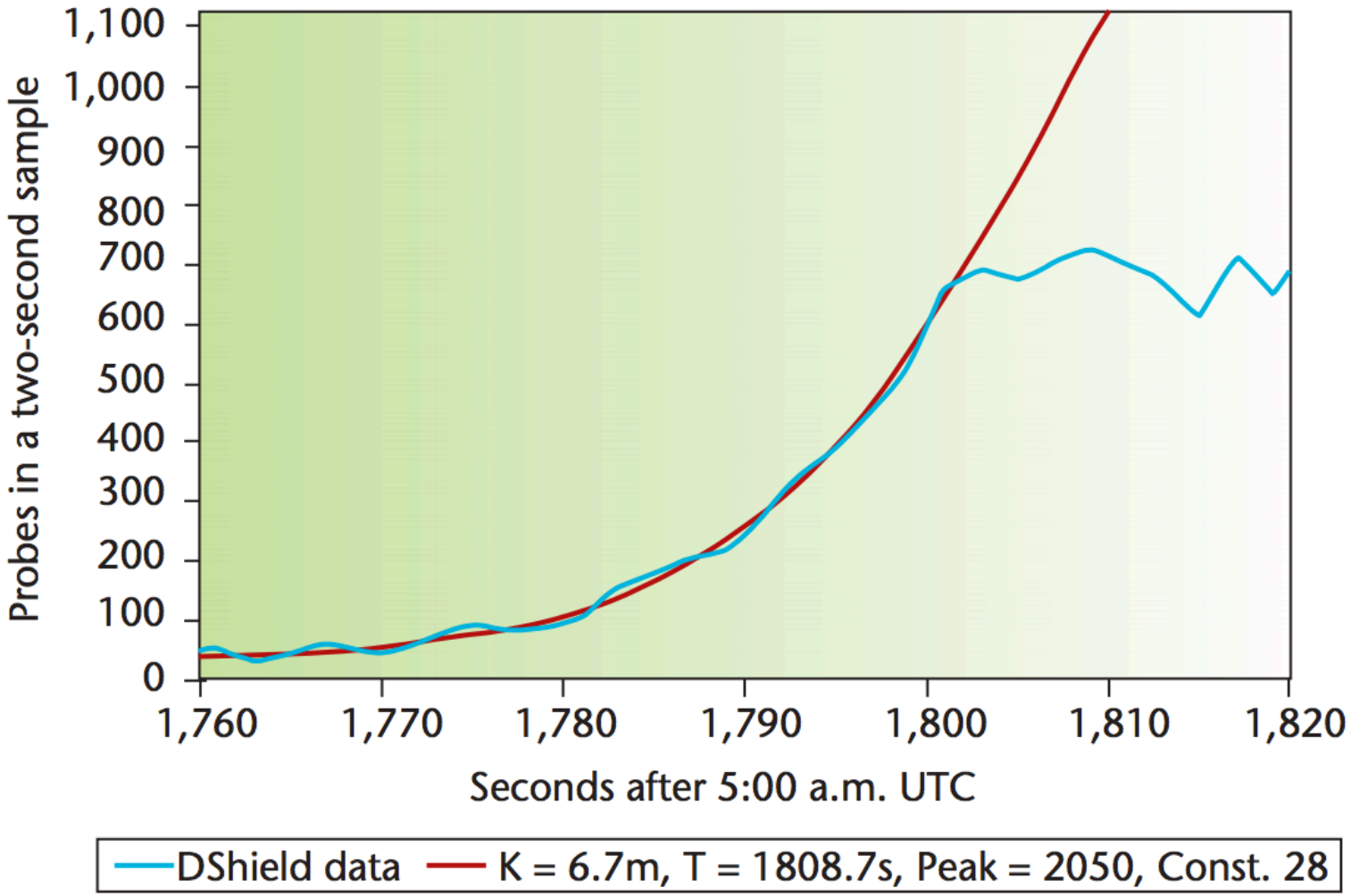
Who are the Attackers?

- Individuals showing off their skills.
- Organized criminals stealing money.
- Hacktivists making a personal or political point.
- Intelligence agencies stealing secrets.
- Terrorists or nation-states trying to inflict serious damage.
- Potential for far worse incidents in the future.
- Let's look at one story from each category.

Slammer Worm: Individual Show Off

- Occurred in 2003.
- Exploited a vulnerability in MS SQL Server.
- Worm data was only 376 bytes! Fit in one packet.
- Handcrafted machine code contained:
  - Data to overflow buffer and gain control
  - Code to find the addresses of needed functions.
  - Code to initialize a UDP socket
  - Code to seed the pseudo-random number generator
  - Code to generate a random address
  - Code to copy the worm to the address via the socket
- Could spew out hundreds or thousands of worms per second from each infected machine.

Slammer Speed and Impact



Source: http://www1.icsi.berkeley.edu/~nweaver/slammer.pdf

Hacktivists

- Picked these guys because they had the NYT website down for two days in 2013
  - Imposed significant costs on the US's best-known newspaper.

SEA's Finest Hour (so far)

That's about a $140 billion spike downward in total value of stock markets.

Source: http://www.ehackingnews.com/2013/04/associated-press-twitter-account-hacked.html

Other Successful SEA Exploits

- Modus operandi is to go after high profile news sites for propaganda value
- BBC
- Huffington Post
- NPR
- Sixty Minutes
- Financial Times
- Washington Post
- Hundreds of websites in total

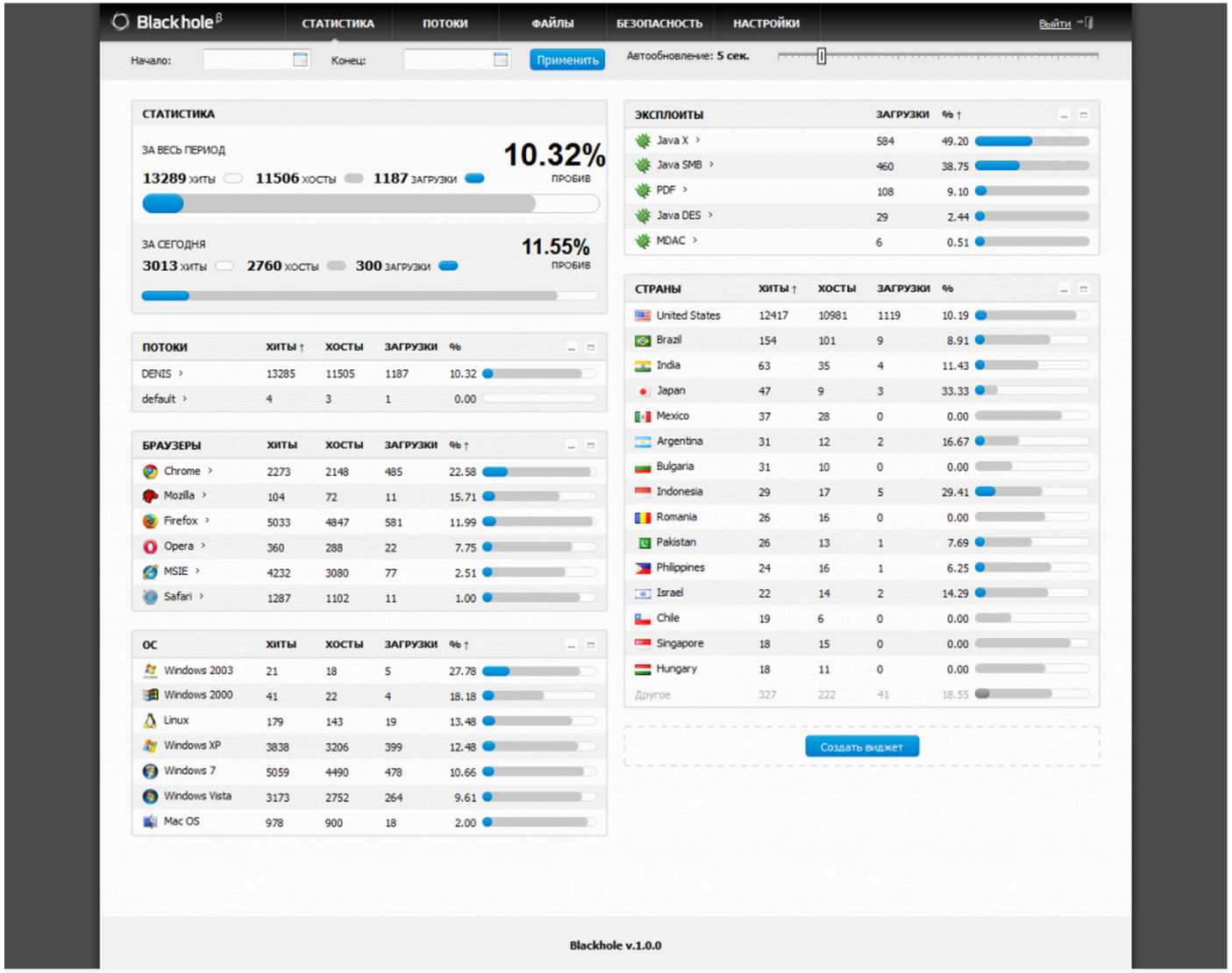
Organized Criminals

- Cybercrime is fairly well organized
  - via underground markets
  - Collaborate together to steal money
- Specialized players take different roles
  - Tool providers (Blackhole, Angler, Zeus, etc)
  - Botnet masters
  - Monetization guys
  - Money mules
- Most in Russia, Ukraine, US, China.

Criminals: Blackhole Exploit Kit

- Circa 2012-2013
- Sophisticated browser exploit framework
  - To help in building botnets of compromised machines
- Typically included as iframes
  - From a legitimate but compromised site
- Checks suitability of source IP
- Serves up some javascript to test suitability of browser
- Exploits browser using suite of exploits
- Keeps track of compromised systems
- Installs moneymaking payload (eg Zeus/derivatives)

Criminals: Blackhole Exploit Kit



Blackhole Author “Paunch”

- 29 year old Russian
- Over 1000 customers
- Was making $50k/mo
- Him with his Porsche:
- Arrested in Dec 2013
  - Russian police

Operation Aurora: Spies

- Large campaign by Chinese PLA unit in 2009
- Revealed by Google
  - stole source code, read gmail of Chinese activists
- Others targeted included: Adobe, Juniper, Symantec, Yahoo, Northrop Grumman, Morgan Stanley
- Dozens to hundreds of western corporations.
- Large scale activity by Chinese intel continues to this day

Operation Aurora: Technical Approach

- Spear Phish email
- Email contained a link to a malicious website
- Website used a zero-day exploit in MS Internet Explorer
- Exploit code downloaded a Trojan exe (RAT)
- RAT obfuscated as an image on wire to avoid AV.
- RAT connected back out for command and control
- Used for lateral spread

Office of Personnel Management

- US govt office that manages background checks for security clearances.
- 21.5 million records believed lost.
- Anonymous govt sources claim it's China.
- Few technical details available.

Stuxnet: Nation State Destruction

The New York Times

Middle East

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 360 Comments

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

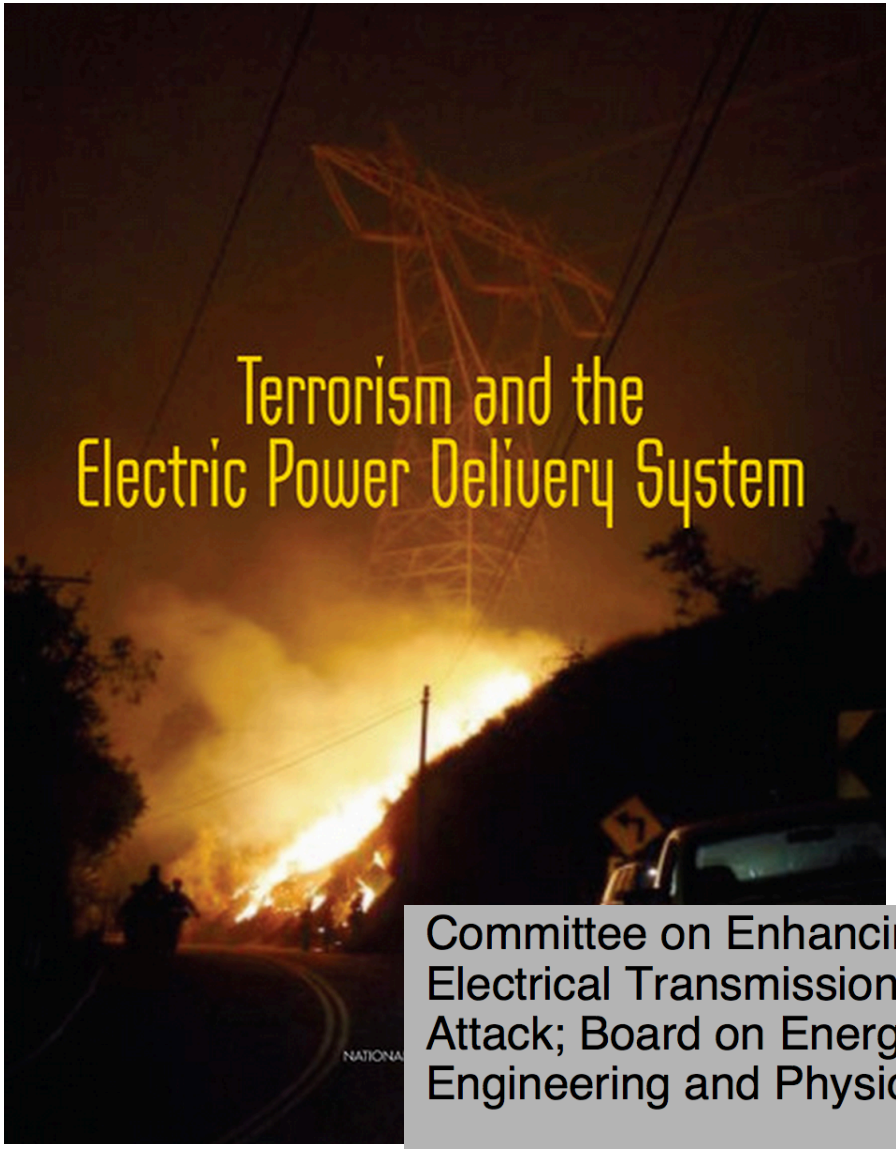
Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

- US/Israeli worm
- NSA and Israeli unit 8200
- 2006-2010 (ish)
- May have set back Iranian nuclear program 18-24 months
- Physically damaged centrifuges

Stuxnet Approach

- Spread on Windows
  - Four zero day vulnerabilities! Plus several known.
  - Installed device drivers using stolen certificates.
  - Identifies systems communicating with particular Siemens industrial control software
- Effect on centrifuges (which spin very fast)
  - Rapidly changed speed
  - Centrifuges self-destruct

Possible Cyberwar Future



The operation of a modern electric power system depends on complex systems of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communication, and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components. Hacking and cyber attacks are becoming increasingly common.

A terrorist attack on the power system would lack the dramatic impact of the attacks in New York, Madrid, or London. It would not immediately kill many people or make for spectacular television footage of bloody destruction. But if it were carried out in a carefully planned way, by people who knew what they were doing, it could deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold.*

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Research Council

Possible Cyberwar Future (2)

- Aurora generator destruction video