Mitigating the Cyber Threat to University Research Data and Intellectual Property (Panel Session)

Joe St Sauver, Ph.D. (joe@uoregon.edu)

Internet2 Global Summit, Denver Colorado

Thursday, April 10th, 2014 8:45-10:00AM

Governor's Square 11

http://pages.uoregon.edu/joe/mitigating/

Disclaimer: all opinions expressed are strictly my own.

A Few Framing Slides For Today's Session

- I'd like to begin by thanking Bob Brammer for the invitation to participate in today's panel.

- My personal perspective in one sentence? We shouldn't be **paranoid** about cyber threats to university research, but **neither can we afford to close our eyes or be naive**.

- That said, there are many international research collaborations that are consensual, mutually beneficial, and invaluable. Our discussion today is **not** about that work.

- Today's discussion is about international nation state threats to sensitive university research, **a theme that we've been hearing about for years.**

The NSHEAB (Created in 2005) and Sensitive University Research

National Security Higher Education Advisory Board

From Wikipedia, the free encyclopedia

The **National Security Higher Education Advisory Board** (NSHEAB) was created by American Federal Bureau of Investigation (FBI) Director Robert S. Mueller III on December 15, 2005.[1] Operated by the FBI and paneled by approximately 20 American university presidents and chancellors, the expressed purpose of the board is "to foster outreach and to promote understanding between higher education and the Federal Bureau of Investigation." The board also facilitates communication between universities and federal authorities on "national priorities pertaining to terrorism, counterintelligence, and homeland security." NSHEAB meets approximately three times yearly and includes representatives from the Central Intelligence Agency and other security agencies.[2]

A stated goal of NSHEAB is to prevent the theft of sensitive research conducted at American universities.[4]

http://en.wikipedia.org/wiki/National_Security_Higher_Education_Advisory_Board

A 2011 Cautionary Report From the FBI

Higher Education and National Security:

The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education

http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-national-security

A NY Times Report From July 2013

Universities Face a Rising Barrage of Cyberattacks

By RICHARD PÉREZ-PEÑA
Published: July 16, 2013

America's research universities, among the most open and robust centers of information exchange in the world, are increasingly coming under cyberattack, most of it thought to be from China, with millions of hacking attempts weekly. Campuses are being forced to tighten security, constrict their culture of openness and try to determine what has been stolen.

Enlarge This Image

Jeff Miller

A storage server at the University of

University officials concede that some of the hacking attempts have succeeded. But they have declined to reveal specifics, other than those involving the theft of personal data like Social Security numbers. They acknowledge that they often do not learn of break-ins until much later, if ever, and that even after discovering the breaches they may not be able to tell what was taken.

http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

The $100,000 "Tin Foil Hat" Question

- Assume you notice a brute force cyber attack against sshd running on a research system at your site.

- You now face a fundamental question...

- Is the hacking attempt that you noticed "just" a spammer (or other monetarily-motivated miscreant), or is that attack actually coming from a nation state interested in the research being done on that system?

- The fact that you noticed a brute force attack may be the first clue that this is likely *NOT* a nation-state attack...

"Routine Hacking" vs "State Sponsored" Attacks

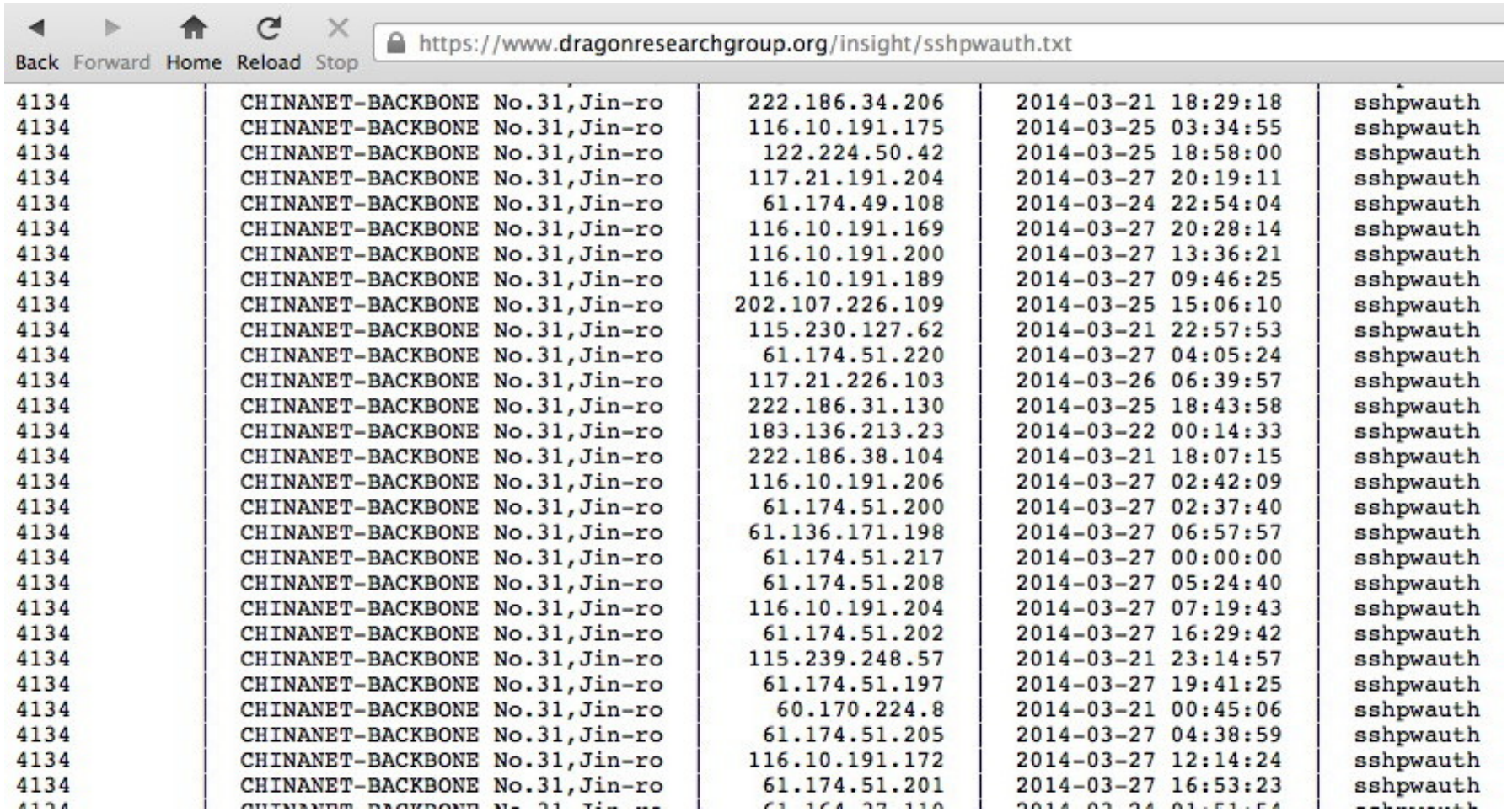
Routine Hacking Attacks

- Motive? **Wants to make $$$$**
- Target: anyone/everyone
- Life cycle: often short
- Sophistication: varies
- Tactics:
  -- Spamming
  -- Phishing
  -- Dropping malware (perhaps via malvertising)
  -- Scan and 'sploit
  -- Extortion (eg Cryptolocker)
  -- Crypto currency mining
- Official response: prosecution by law enforcement (sometimes)

State Sponsored Attack

- Motive? **Wants specific intel**
- Target: specific institutions, departments, or individuals
- Life cycle: often long
- Sophistication: often high
- Tactics:
  -- "Spear phishing"
  -- "Watering hole" attacks
  -- Attacking partitioned networks via removable media (thumb drives, etc.)
  -- Insider threat
- Official response: handled via counterintelligence agencies (sometimes)

ARE Cyber Attacks Taking Place? Yes. Example: IPs Observed Doing SSH Brute Force Attacks…



4134	CHINANET-BACKBONE No.31,Jin-ro	222.186.34.206	2014-03-21 18:29:18	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.175	2014-03-25 03:34:55	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	122.224.50.42	2014-03-25 18:58:00	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	117.21.191.204	2014-03-27 20:19:11	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.49.108	2014-03-24 22:54:04	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.169	2014-03-27 20:28:14	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.200	2014-03-27 13:36:21	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.189	2014-03-27 09:46:25	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	202.107.226.109	2014-03-25 15:06:10	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	115.230.127.62	2014-03-21 22:57:53	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.220	2014-03-27 04:05:24	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	117.21.226.103	2014-03-26 06:39:57	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	222.186.31.130	2014-03-25 18:43:58	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	183.136.213.23	2014-03-22 00:14:33	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	222.186.38.104	2014-03-21 18:07:15	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.206	2014-03-27 02:42:09	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.200	2014-03-27 02:37:40	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.136.171.198	2014-03-27 06:57:57	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.217	2014-03-27 00:00:00	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.208	2014-03-27 05:24:40	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.204	2014-03-27 07:19:43	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.202	2014-03-27 16:29:42	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	115.239.248.57	2014-03-21 23:14:57	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.197	2014-03-27 19:41:25	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	60.170.224.8	2014-03-21 00:45:06	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.205	2014-03-27 04:38:59	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	116.10.191.172	2014-03-27 12:14:24	sshpwauth
4134	CHINANET-BACKBONE No.31,Jin-ro	61.174.51.201	2014-03-27 16:53:23	sshpwauth

https://www.dragonresearchgroup.org/insight/sshpwauth.txt

Those IPs Likely Represent "Botted Hosts"...

- A botted host is usually an unpatched Windows PC that has gotten infected with malicious software ("malware"). There are millions of botted hosts on the Internet at any given time.

- Once infected with malware, a remote attacker can use botted systems as if they were his or her own, including using them for mundane things (such as spamming)... or for hacking/cracking sensitive research-related systems.

- While the NY Times report mentioned attacks from China, there are networks with problematic levels of botted hosts in many countries (including China) but also including India, Vietnam, Belarus, Taiwan, Kazakhstan, Germany, etc.

Bots Are Located In Many Countries, But Who Knows The Nationality/Allegiance of Those Who May Be Conducting Attacks Through Those Hosts?

load Stop cbl.abuseat.org/asn.html

ASN	Listings	%total	% Total Listings	%cumulative Total Listings	Rank
Total	7789816	100			
AS9829 sancharnet.in IN	366831	4.71	4.71	4.71	1
AS4134 chinanet.cn.net CN	362337	4.65	4.65	9.36	2
AS45899 vnnic.net.vn VN	333344	4.28	4.28	13.64	3
AS6697 belpak.by BY	193716	2.49	2.49	16.13	4
AS3462 hinet.net TW	145421	1.87	1.87	17.99	5
AS4837 cnc-noc.net CN	121524	1.56	1.56	19.55	6
AS9198 online.kz KZ	107908	1.39	1.39	20.94	7
AS3320 dtag.de DE	105066	1.35	1.35	22.29	8
AS45595 ptcl.net.pk PK	104671	1.34	1.34	23.63	9
AS200080 DEL BG	97920	1.26	1.26	24.89	10

List of spamming botted hosts per ASN, http://cbl.abuseat.org/asn.html

Another Factor: Higher Education Is Often (At Most) A Secondary Focus for Espionage…

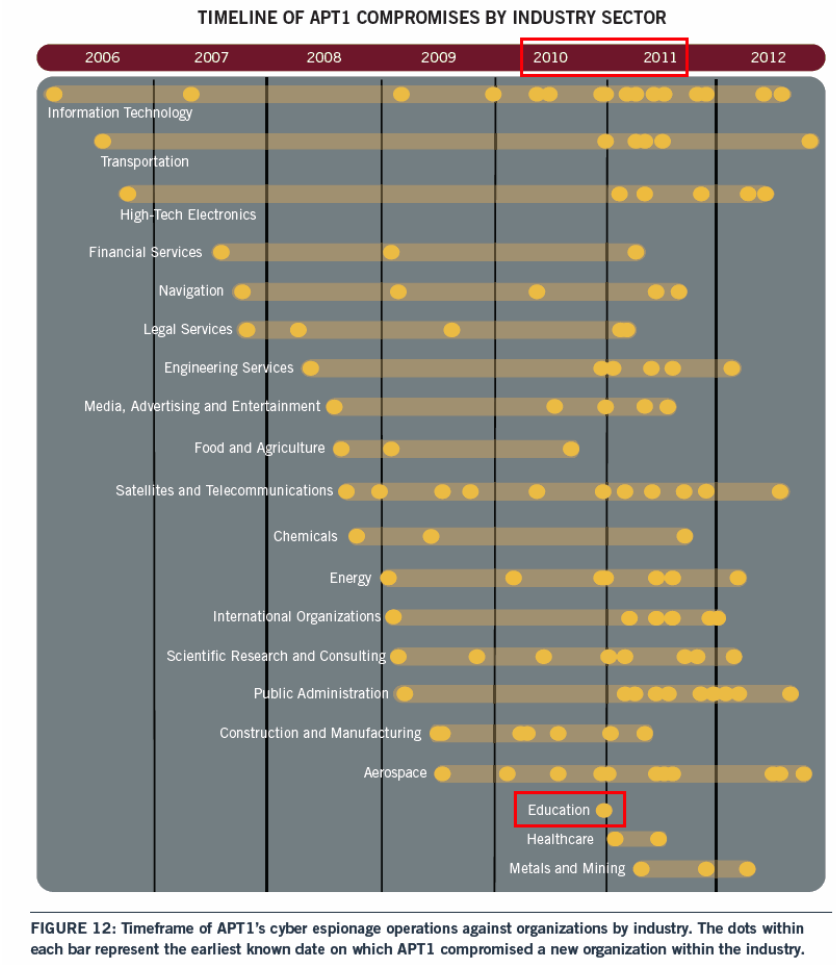


FIGURE 12: Timeframe of APT1's cyber espionage operations against organizations by industry. The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry.

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf page 23.

One Reason Why Universities Aren't Much Of A Priority for Espionage: We're Pretty Open

- Most universities aren't much of a target for cyber espionage because most of the research we do is fundamental, and isn't classified, proprietary, or otherwise sensitive.

- In fact, most university researchers routinely publish their findings and share their data as a matter of policy. If you're interested in it, just look it up in a peer-reviewed journal or attend the open meetings where that research often will get shared.

- After all, universities are *supposed* to create and disseminate research-related knowledge, right?

"A Vision Statement for the University's Role in Dissemination"

- "The creation of new knowledge lies at the heart of the research university and results from tremendous investments of resources by universities, federal and state governments, industry, foundations, and others. The products of that enterprise are created to benefit society. In the process, those products also advance further research and scholarship, along with the teaching and service missions of the university. Reflecting its investments, **the academy has a responsibility to ensure the broadest possible access to the fruits of its work both in the short and long term by publics both local and global.**

  "Faculty research and scholarship represent invaluable intellectual capital, but the value of that capital lies in its effective dissemination to present and future audiences. **Dissemination strategies that restrict access are fundamentally at odds with the dissemination imperative inherent in the university mission."** [2009]

- http://www.aau.edu/WorkArea/DownloadAsset.aspx?id=8320

The NSF's Expectations for Research Sharing

- a. Investigators are expected to promptly prepare and submit for publication, with authorship that accurately reflects the contributions of those involved, all significant findings from work conducted under NSF grants. Grantees are expected to permit and encourage such publication by those actually performing that work, unless a grantee intends to publish or disseminate such findings itself.
- b. Investigators are expected to share with other researchers, at no more than incremental cost and within a reasonable time, the primary data, samples, physical collections and other supporting materials created or gathered in the course of work under NSF grants. Grantees are expected to encourage and facilitate such sharing. [continues]

[www.nsf.gov/pubs/policydocs/pappguide/nsf11001/aag_6.jsp#VID4

There *Are* A Few Exceptions...

- Not *all* research data can (or should!) be freely shared. The most common exceptions are probably:

  -- Classified research done under government contract (assumed to NOT be done on most campuses, and thus out of scope for today's campus-focused discussion)

  -- Research involving dual use technologies subject to specific export control limitations

  -- Commercially-valuable applied research

  -- Research involving human subjects' private data

  -- Can you think of other examples?

Assuming You DO Have Sensitive Research That Needs To Be Specially Protected…

- What SHOULD you be doing to protect sensitive research data and mitigate the risk of targeted cyber attacks beyond what you may already be routinely doing?

- How is sensitive RESEARCH data different than other sensitive information that may also be on campus, including:

  -- confidential educational or personnel records?
  -- protected health-related information?
  -- payment card-related information?
  -- other sensitive non-research data?