Internet2 Security Update
Spring 2011 Member Meeting

Joe St Sauver, Ph.D.
joe@internet2.edu or joe@oregon.uoregon.edu
Internet2 Nationwide Security Programs Manager

3:00-4:00PM Tuesday, April 19th, 2011
Internet2 Member Meeting, Arlington VA

http://pages.uoregon.edu/joe/s2011-sec-update/

Welcome!

- Welcome to the 2011 Security Update session, which is being netcast live.
- We're going to have three speakers today, each covering 15-18 minutes of material, with some time at the end for questions.
- I'm Joe St Sauver, Internet2's Nationwide Security Program Manager, and I'll lead off today session.
- Next, we'll have Doug Pearson, Technical Director for the REN-ISAC.
- Finally, we'll have Chris Misra, head of Salsa, Internet2's Security Advisory Committee.
- To ensure we stay on track this afternoon, we'll hold questions until all three speakers have finished their presentations.

Other Security or Security-Related Sessions

- Before I dive into my material, I wanted to mention that we're fortunate to have had a *ton* of great security-related sessions during this week's meeting...

- **Monday, April 18th (Yesterday)**

  -- *Cybersecurity and the Social, Behavioral and Economic Sciences*, David Croson (NSF), April 18th, 1:15-2:30, Salon B

  -- *Security in the Broadband Network,* Artur Barczyk (Cal Tech), Chris Janson (Ciena), and Bob Kimball (Ciena Government Solutions), April 18th, 3:00-4:00, Salon B

  -- *IPv6 Security Planning Panel*, Schuman Huque (Penn), Mike Lococo (NYU), Joe Klein, and myself, April 18th, 4:30-5:30, Salon B

- **Tuesday, April 19th (Today)**

  -- *Salsa Disaster Planning and Recovery BoF,* 7:30-8:30, Jefferson
  -- *Philosophical Reflections on Network Security,* Marc Wallman (NDSU), 8:45-10:00, Salon C
  -- *Balancing Risk and Opportunity for an Institutional Groups Service*, Michael Brogan (UW), 8:45-10:00, Salon B
  -- *Salsa Advisory Group Lunch*, 12:00-1:00, Alexandria
  -- *DNS: Don't Call It Insecure Any More,* Leif Johansson (SUNET/NORDUnet), 1:15-2:30, Salon C
  -- *Isolating Video Networks for Management and Security,* Jeff Egly & Kevin Quire (UEN), 4:30-5:30, Salon A
  -- *Physical Security of Advanced Network and Systems Infrastructure*, Joe St Sauver (I2/UO), 4:30-5:30, Salon C
  -- *Authorization and Intelligent Design,* Barton (Chicago), Dopirak (CMU), Hazelton (Madison) and Hedberg (Umea), 4:30-5:30, Salon H

- **Wednesday, April 20th (Tomorrow)**

  -- *DNSSEC BoF,* 7:30-8:30, Salon J
  -- *Oracle IDM Integration BoF,* Rob Carter and Shilen Patel (Duke), 7:30-8:30, Jackson
  -- *Cutting Edge 2-Factor AuthN Using Smart Phones,* Teunissen, van Dijk and van Rijswijk (SURFnet), 1:15-2:30, Salon D
  -- *Applications, Middleware & Services Advisory Council Open Meeting* (the Security Area is part of AMSAC's portfolio), 4:30-5:30, Salon B

- THANK YOU to everyone who has delivered or participated in one or more of these security-related sessions!
- Now let's begin by talking a little about how security fits into the big picture for Internet2.

1. Risk Management, Business Resilience, And The Path Forward for Internet2

"The Path Forward"

- Those of you who had the pleasure to hear David Lambert, Internet2's new President and CEO, at the Fall Member Meeting in Atlanta, will no doubt remember his challenging charge to the community in his session, "The Path Forward," see http://www.internet2.edu/presentations/fall10/20101102-path-forward-lambert.pdf
- He outlined six challenges that our community faces:
  -- The impact of globalization
  -- Science/research moving to large-scale, distributed, projects
  -- The impact of for-profit providers
  -- Lifelong learning, and the critical role of community and vocational colleges
  -- Decreased public funding and increased educational costs
  -- **Risk management and business resiliency requirements**
- We believe that last item, bolded above, relates most closely and directly to system and network security.

Security and Risk Management

- One measure of the close relationship between security, risk management, and business resiliency can be seen in simple things, such as how often they're lumped together at community meetings. Just to mention a couple of examples, if you attend the huge **Interop** IT trade show, one of their tracks is called the "**Information Security and Risk Management Conference Track,**" and **Gartner's** offering a "**Security and Risk Management Summit**" here in the DC area this summer.
- IBM, another long time security-thought leader, as part of their security and business resilience practice, talks about what "SmarterSecurity&Resilience" means to them, e.g., an intelligent approach to risk management that reveals opportunities for innovation, including moving from "experience and react" to "anticipate and adjust."
- The link between security and risk management is thus well established, and a mainstream one.

Risk Management's Potential… and Pushback

- Risk management is also of great interest because of its potential to rationalize security investments and achieve significant security cost containment -- BUT probabilistic security models have also seen significant pushback from the community.
- For example, just this year, the National Academies released an unclassified public summary report relating to one very serious risk analysis, "Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex," www.nap.edu/catalog.php?record_id=13108 That report summary said in part:

  > *RECOMMENDATION 3-1: The committee advises* ***against the use of probabilistic risk assessment (PRA)*** *in designing security for the DOE nuclear weapons complex at this time. However, the committee recommends the use of some tools and techniques traditionally associated with PRA to improve NNSA's understanding of the full spectrum of risks to the complex.* [emphasis added]

- Why might some advise against probabilistic risk assessment?

Economic (Ir)Rationality and The Perception of Risk

- Its well known that PRA tries to impose "economic rationality" on potentially *ad hoc* decision making processes.
- For example, consider a greatly simplified hypothetical vulnerability that might occur once and only once, and which has a potential economic impact of $20,000 if it does occur. Let's assume that we "know" we have a 50-50% chance of that vulnerability happening. If trying to mitigate that vulnerability costs ***more*** than $10,000 ($20,000 * 0.5=$10,000), should we do it? Or should we just decide to knowingly "assume that risk?"
- Now, what about a potential "university-killing" billion dollar risk with a 1-in-100,000 chance of occurring? ***Should*** we ***still*** spend no more than $1,000,000,000 * 0.00001 = $10,000 to abate *that* risk? Or should we spend ***more*** on that sort of risk (given its potential outcome)? Or should we spend ***less*** on that risk (given its low probability of actually occurring)?

Another Problem With PRA: Unknown Unknowns

- Recall Donald Rumsfeld's famous quote from a news briefing in February 2002:

> *"As we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know."*

- Another place where PRA runs into difficulty is when it comes to assigning likelihoods to "unknown unknowns,", and when it comes to trying to correctly quantify high-impact but low-likelihood events.

University CIOs: Security And Related Areas Remain Key Institutional Challenges

- Every year, Educause surveys higher education CIOs, asking them to pick the most-important issues from a list of twenty-seven possibilities. The most recent results are:

1. Funding IT
2. Admin/ERP/Information Systems
3. **Security**
4. Teaching/Learning with Technology
5. **Identity/Access Management**
6. **(tie) Disaster Recovery/Business Continuity**
6. (tie) Governance, Organization and Leadership
7. Agility, Adaptability, and Responsiveness
8. Learning Management Systems
9. Strategic Planning
10. Infrastructure/Cyberinfrastructure

Security: A Broad Topic

- So, when we talk about security, we tend to treat it as a broad topic. When we look at the Educause CIO issues survey, in addition to the "security" topic in third place, we'd also highlight the closely related areas of Identity/ Access Management, and Disaster Recovery / Business Continuity. **No other area comes close to security's level of higher education IT leadership "mindshare," so its wonderful that Internet2 and our community continue to recognize the importance of security and closely related topic areas.**
- We must also acknowledge that we're in the Washington DC metro area today, and cyber security, identity management and business continuity are "front and center" on the federal agenda, just as they are on ours.
- Just to mention a couple of examples from the last month…

The Federal Cybersecurity Agenda

- At the end of March, the Whitehouse issued **Presidential Policy Directive 8 (PPD-8)**, entitled, "National Preparedness," (see http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm). The fact that this is only the 8th such directive from the Obama administration, underscores its potential impact and importance. That policy is aimed at "strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, **cyber attacks**, pandemics, and catastrophic natural disasters."
- And just last Friday, on April 15th, 2011, the Administration also released its **National Strategy for Trusted Identities in Cyberspace** (NSTIC), see http://www.nist.gov/nstic/ The congruence between what the Administration is recommending, and the work that's already been done by the Internet2/Incommon/Shibboleth community is striking.

Cybersecurity at the Department of Education

- Another example of how cyber security has been on the federal radar could be seen in the keynote address that Richard Gordon, CIO for the US Department of Education, delivered at the 2011 Educause/Internet2 Security Professionals Meeting in San Antonio earlier this month.
- In his remarks, Mr. Gordon described the Department's plans to improve the security of PII that may have been collected as part of the Federal Financial Aid program, including discussing the creation of an advisory board.
- Thus, even if you don't care about PPDs relating to cyber security, or major efforts to redesign the nation's cyber identity management infrastructure, I think *every* university cares about "meat and potato security issues" such as protecting federal financial aid data and institutional personally identifiable information.

Much Work Remains To Be Done

- If I can sum up this first half of my talk, it would be to say that:

  -- security remains an important and popular area for the higher education community
  -- our federal friends and colleagues share our interest in improving cyber security
  -- it is wonderful to see Internet2 continuing to recognize and support work in this vital area

- So now let's also talk a little about what's currently happening in some security-related areas.

2. What's Currently Happening In Some Security-Related Areas

(a) The InCommon Certificate Service

- The Internet2 InCommon Certificate Service offers unlimited SSL certificates for one fixed fee for all campus servers and domains, including all domains owned by the school (such as professional organizations or athletic sites, including any .org, .com, .net or other domains).
- This includes unlimited Domain Validation SSL certs and Extended Validation ("green bar") certs, and personal certs for signing and encryption (code-signing certs are coming)
- Trust anchors are in all major browsers and other clients
- Campus staff create and control certificates through the a GUI Certificate Manager interface or via an API
- For more info, see http://www.incommon.org/cert/ (that site has a very helpful FAQ, and also has information about how to subscribe, participation costs, etc.)

Who's Currently Participating? 102 Sites...

Arizona State University California Institute of Technology; California Maritime Academy; California Polytechnic State University-San Luis Obispo; California State Polytechnic University, Pomona; California State University, Bakersfield; California State University, Channel Islands; California State University, Chico; California State University, Dominguez Hills; California State University, East Bay; California State University, Fresno; California State University, Fullerton; California State University, Long Beach California State University, Los Angeles; California State University, Monterey Bay; California State University, Northridge; California State University, Office of the Chancellor; California State University, Sacramento; California State University, San Marcos; California State University, Stanislaus; California State University San Bernardino; Carleton College; Clemson University; Columbia University; Drexel University; Duke University; Emory University; Fort Lewis College; George Mason University; Georgetown University; Humboldt State University; Indiana Institute of Technology; Indiana University at Bloomington; Internet2; Iowa State University; James Madison University; Lafayette College; Loyola University Maryland; Medical University of South Carolina; Miami University; Michigan Technological University; Northwestern University; Ohio Northern University; Ohio University Main Campus; Penn State (The Pennsylvania State University); Princeton University; Purdue University Main Campus; Regis University; Rice University; San Diego State University; San Francisco State University; San Jose State University; Skidmore College; Sonoma State University; Southern Methodist University; Texas Tech University; The Moody Bible Institute of Chicago; The Ohio State University; The University of Montana; University of Alaska Statewide System; University of California, Office of the President; University of California-Berkeley; University of California-Davis; University of California-Los Angeles; University of California-San Diego; University of California-San Francisco; University of Central Florida; University of Chicago; University of Cincinnati Main Campus; University of Florida; University of Illinois at Urbana-Champaign; University of Iowa; University of Maryland Baltimore County; University of Massachusetts; University of Minnesota-Twin Cities; University of Missouri System; University of Nebraska - Lincoln; University of North Carolina At Greensboro; University of Richmond; University of South Florida; University of Texas at Arlington; University of Texas at Austin; University of Texas At Brownsville; University of Texas at Dallas; University of Texas at El Paso; University of Texas at San Antonio; University of Texas At Tyler; University of Texas Health Science Center At Houston; University of Texas Health Science Center At San Antonio; University of Texas M. D. Anderson Cancer Center; University of Texas Medical Branch At Galveston; University of Texas of the Permian Basin; University of Texas Southwestern Medical Center at Dallas; University of Texas System; University of Texas-Pan American; University of Vermont; University of Virginia; University of Wisconsin Madison; University of Wisconsin-Whitewater; Villanova University; Virginia Commonwealth University; and Whitman College.

[Source: http://www.incommonfederation.org/cert/subscribers.cfm]

CRLs and OCSP

- A recent certificate-related incident highlighted one cert security issue you may want to think about, and that's how browsers and user systems handle revoked SSL certificates.
- Certificate Revocation Lists (RFC5280) and the Online Certificate Status Protocol (RFC2560) are supposed to be the basis for signaling the revocation status of certs. Unfortunately, some browsers (such as some versions of Safari) do not do CRL and OCSP checking by default.
- If revocation checking isn't done, users risk trusting a revoked certificate, which is generally a pretty bad idea.
- You may want to encourage your users to consider using browsers that do support OCSP and CRLs by default (such as current versions of Firefox). You should also encourage users to apply all relevant patches!

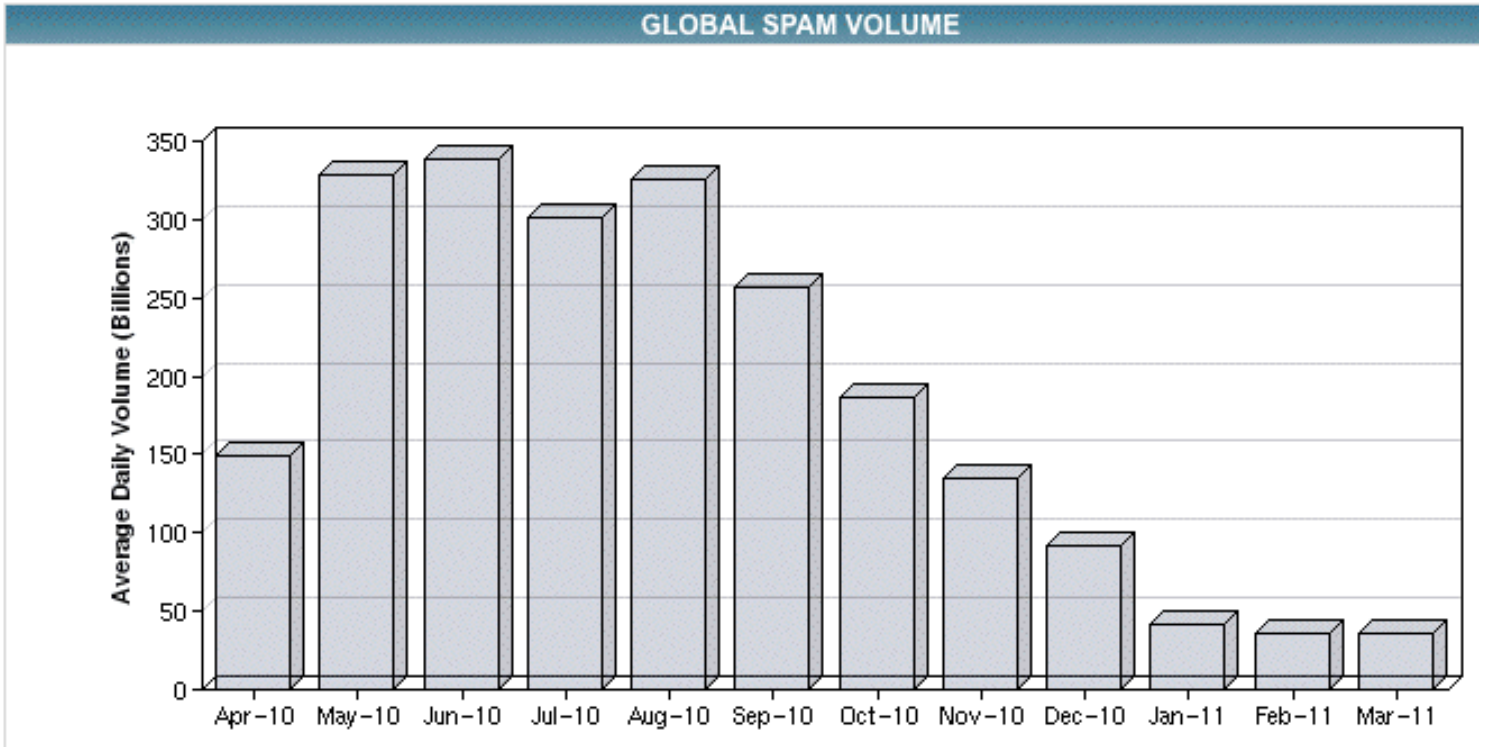
(b) Botnets: Rustock, Coreflood, etc.

- **Rustock**, generally believed to be the #1-ranked botnet worldwide, with at least 1.7 million infected PCs, was successfully taken down by Microsoft, Pfizer, FireEye and researchers from the University of Washington as part of an effort known as "Operation b107"

- The venerable and tenacious **Coreflood** botnet (with estimates of over 2.3 million infected PCs), was successfully taken down by FBI agents from Connecticut. See www.justice.gov/opa/pr/2011/April/11-crm-466.html It is particularly noteworthy that the FBI received permission not just to take down the botnet command and control hosts, but also to turn off the bot software running on the hosts participating in that botnet (often botnet command and control hosts are "decapitated," but the botted hosts are then left infected, waiting for a new botherder to come along and take them over).

What Bots Getting Taken Down Means To You

- While many major bots remain up, work on major botnets over the last half year directly translates to nearly an **order of magnitude** less email spam traffic worldwide…



Source: http://www.senderbase.org/home/detail_spam_volume

Botted Hosts in the US

- One of the pre-eminent sources of data on botted hosts is the "Composite Block List." In addition to doing a great job when it comes to blocking a lot of spam, it also provides some very helpful summary stats (thank you CBL folks!)
- http://cbl.abuseat.org/country.html for instance, breaks out botted hosts by country.
- There are currently 117,853 known botted hosts in the US, and that may seem like a lot in absolute terms, but when you think about that as a percentage, you can see that means that **only 0.01% of all US IP addresses are currently detected as botted** -- that's **one one-hundredth of one percent!**
- In my opinion that's an amazing accomplishment for security professionals here in the United States. You don't see that sort of thing very often...

It's *Not* Time To Let Your Guard Down, Though

- While bot levels are way down in the US, ironically that may spur cyber miscreants to work hard to create *new* replacement botnets. Therefore, we urge you to be doubly vigilant when it comes to malware that is, or may soon be, in circulation.
- Two particularly useful tools in the fight against malware:
  -- **Team Cymru's WinMHR**, a free program that scans your PC's files for hashes that may be flagged by any of many A/V vendors as malicious. (See http://www.winmhr.com/)
  -- **Secunia PSI (and CSI)** are programs that you can run on your Windows PCs to identify out-of-date software from third party vendors such as Adobe, Apple, etc. (See http://secunia.com/vulnerability_scanning/)
- Sometimes, though, even **knowing** that you need to update, doesn't mean that you'll be **able** to do so.

Sidebar: "Ancient" But Still In Wide Use

- Now that Apple has focused on Intel processors for the Mac, what about faculty, students and staff using older Macs with PowerPC (PPC) chips? You should recognize that increasingly, **critical software updates are NOT getting provided for older Macs using the classic PPC architecture.**
- For example, the Mac OS X 10.6 ("Snow Leopard") operating system has not been made available for PPC Macs (10.5.8 was the end of the line for them).
- The Firefox 4.x browser is also not available for PPC Macs, likewise Google Chrome and Opera 11.
- Adobe Flash Player 10.2 for Mac is not available for PPC.
- **The writing certainly appears to be on the wall. Has your site declared all PPC Macs end-of-life? *Should you?***
  If not, what's your strategy for keeping those systems safe when security updates are no longer available?
- And what's your plan for retiring old **Windows XP boxes?**

Looking Overseas For a Moment: Bots In China

- For many years, many of us in the security community worried about the number of compromised systems we were seeing in China, and the spam (and other unwanted network traffic) that was getting emitted from those botted hosts.
- Recently China has made great progress in dealing with this security issue.
- While China still has 213,754 botted hosts listed on the CBL, those systems represent only **0.073% of all Chinese IPs.** China thus isn't 100% clean, any more than we are here in the United States, **but they *have* made tremendous progress when it comes to dealing with botted hosts, and we salute their achievement!**
- Unfortunately, not all countries have their botnet problems equally well in hand. For example, consider India…

Bots in India

- **1,144,320 botted hosts in India were listed on the CBL on April 15th, 2011, the most of <u>any</u> country, representing 15.59% of all hosts listed on the CBL as of that date.**
- Even normalizing for the large number of Indian IP addresses in use, that still translates to an **infection rate of 4.392% of all Indian systems, or over 400 times the infection level here in the United States.**
- Why are PCs in India getting botted at that rate? Is there anything we can or should do about this issue, perhaps as part of Internet2's international activities?
- Shouldn't Microsoft's classic recipe for securing home PCs as used here in the US work in India, too? (Just to review, their recipe is: install a trustworthy antivirus and antispyware program, update your software regularly, never turn off your firewall, use strong passwords and keep them secret, and use flash drives cautiously)

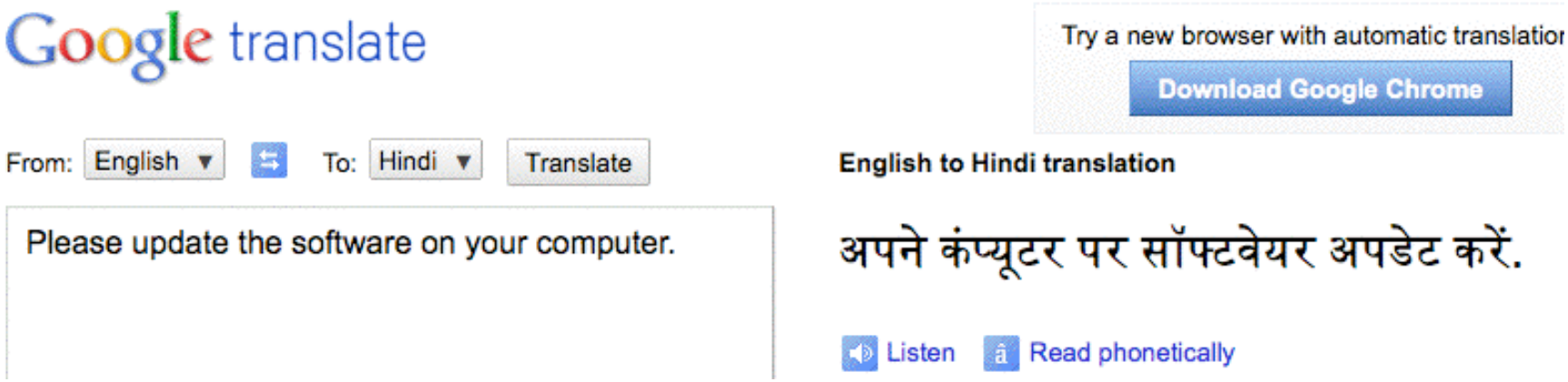
Security and The Languages of India

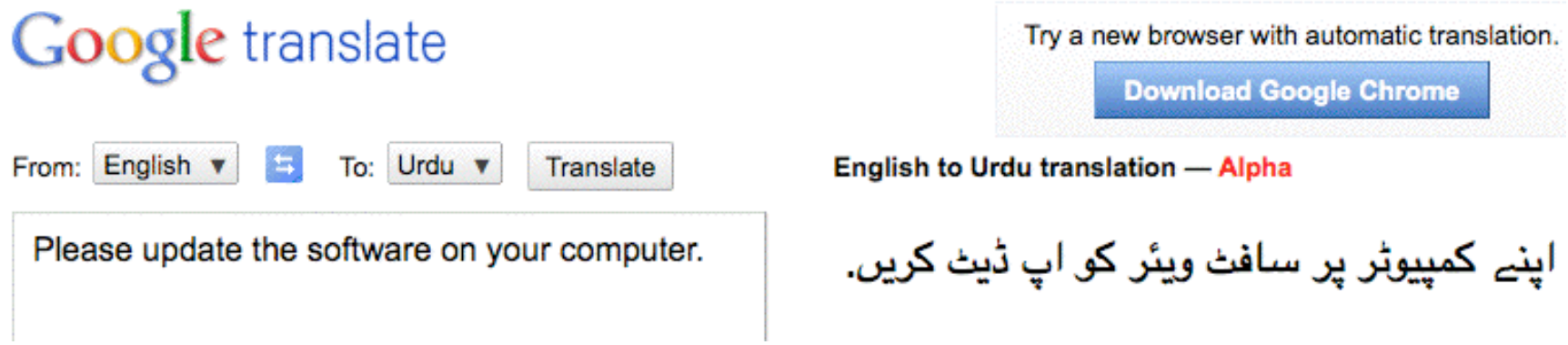
- Part of the issue may be a matter of languages – while the popular misperception is that all those who live in India speak Hindi or English, in reality, India is a land where many regional languages predominate. Only around 40% of Indians have any Hindi and only a few percent of Indians actually use English, see for example http://news.bbc.co.uk/2/hi/8365631.stm
- Many Indians use other, less-well-known, South Asian languages such Assamese (1.3%), Bengali (8.1%), Gujarati (4.5%), Kannada (3.7%), Maithili (1.2%), Malayalam (3.2%), Marathi (7%), Oriya (3.2%), Punjabi (2.8%), Tamil (5.9%), Telugu (7.2%), or Urdu (5%). (See: http://www.cia.gov/library/publications/the-world-factbook/geos/in.html).
- Of course, even a language that's used by "just" 1% of India's population still represents a language used by nearly 12 million people!
- For comparison, there were a little over 28 million Spanish-speakers in the US in 2000, and there are just under 7 million Canadians who speak French.

Localized Advice and Security Tools

- So, what may be needed in India is appropriately localized security advice and appropriately localized security software tools. Do we have members of the Internet2 community, either here in Arlington or participating via netcast, who might want to work on this issue?
- I'd note for our corporate members in particular that the market for appropriately localized security products in India should be huge, but I must also acknowledge that:
  -- expertise in less common South Asian languages may be scarce (and competition for good candidates intense)
  -- South Asian languages use non-Roman alphabets, and not all development environments may support them (but see http://tdil.mit.gov.in/)
- Bottom line: this may be a challenging project to undertake, but one that I think we should consider.

What About Google Translate? Yes, It *Does* At Least Do Hindi (and Now Even Urdu)





Question: any native Hindi or Urdu speakers in the audience? What do you think?

(c) Disaster Recovery and Japan

- Finally, we were all stunned as we watched the devastation inflicted on Japan by one of the largest earthquakes in history, followed by an extreme tsunami and then problems at the Fukushima Daiichi nuclear complex.
- I know I speak for everyone when I say that our hearts and prayers go out to all our Japanese colleagues and friends. I hope you will all consider donating generously to the Red Cross to help those who have been affected.
- The Internet2 Salsa Disaster Recovery working group met just this morning to begin capturing lessons learned from the recent Japanese disaster and to think a little about how the Internet2 community might best prepare itself to react should we ever suffer a similar disaster here in the United States. You can see some initial thoughts on this at http://tinyurl.com/salsa-dr-japan-tragedy

That's About All I Have Time For Today

- Doug, would you like to bring folks up to date on what's been happening with the REN-ISAC?