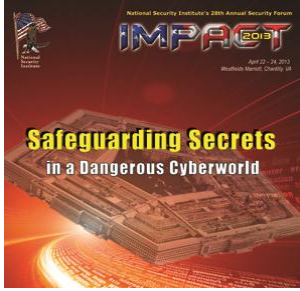
National Security Institute
28th Annual
IMPACT 2013 Security Conference



How the Cybersecurity Executive Order Will Impact You

April 23, 2013

Jamie Barnett
Rear Admiral, USN (Retired)
Attorney at Law
Partner, Venable LLP
Co-Chair, Telecom

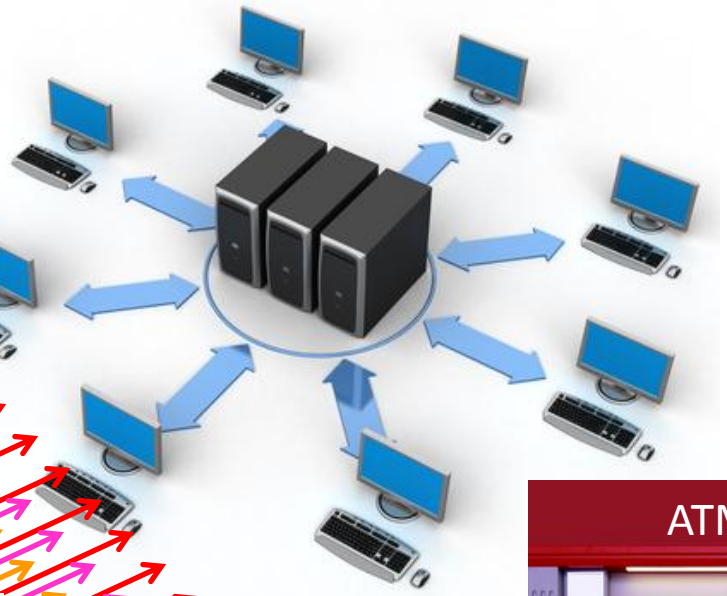
VENABLE® LLP

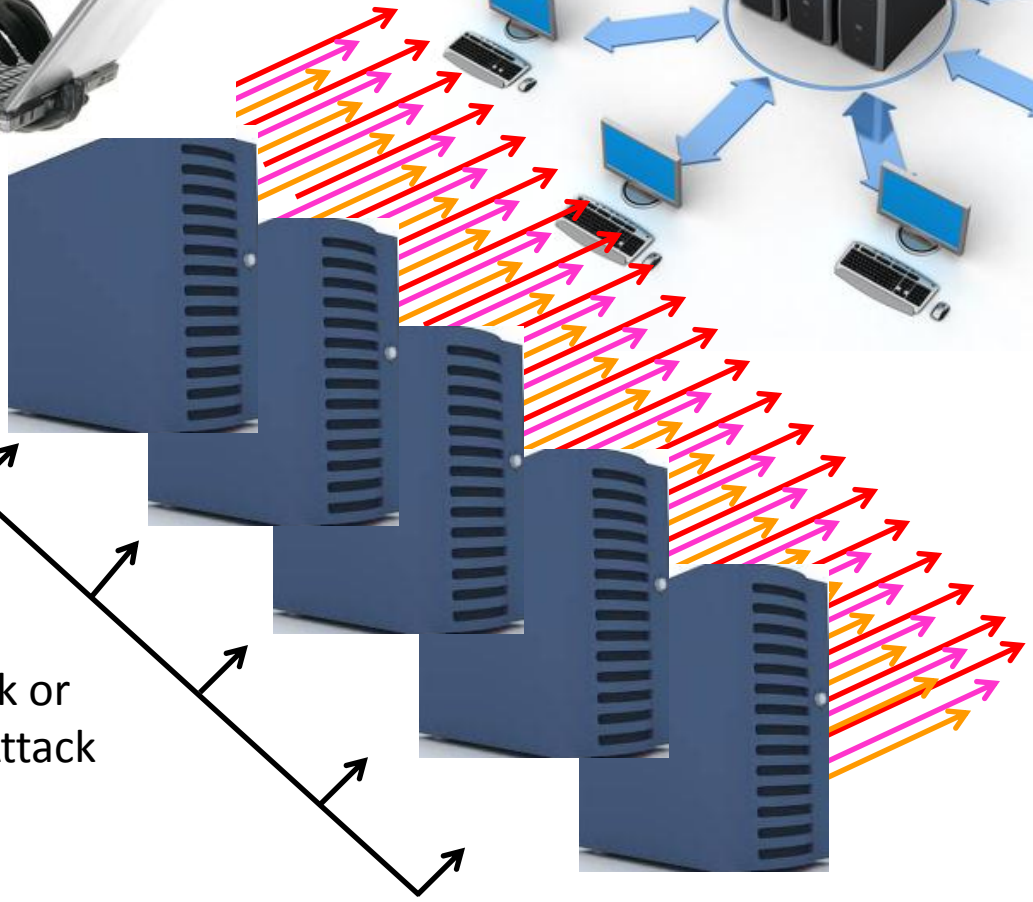
VENABLE LLP

The Daily News

VENABLE LLP

Distributed Denial of Service Attacks Against Banks





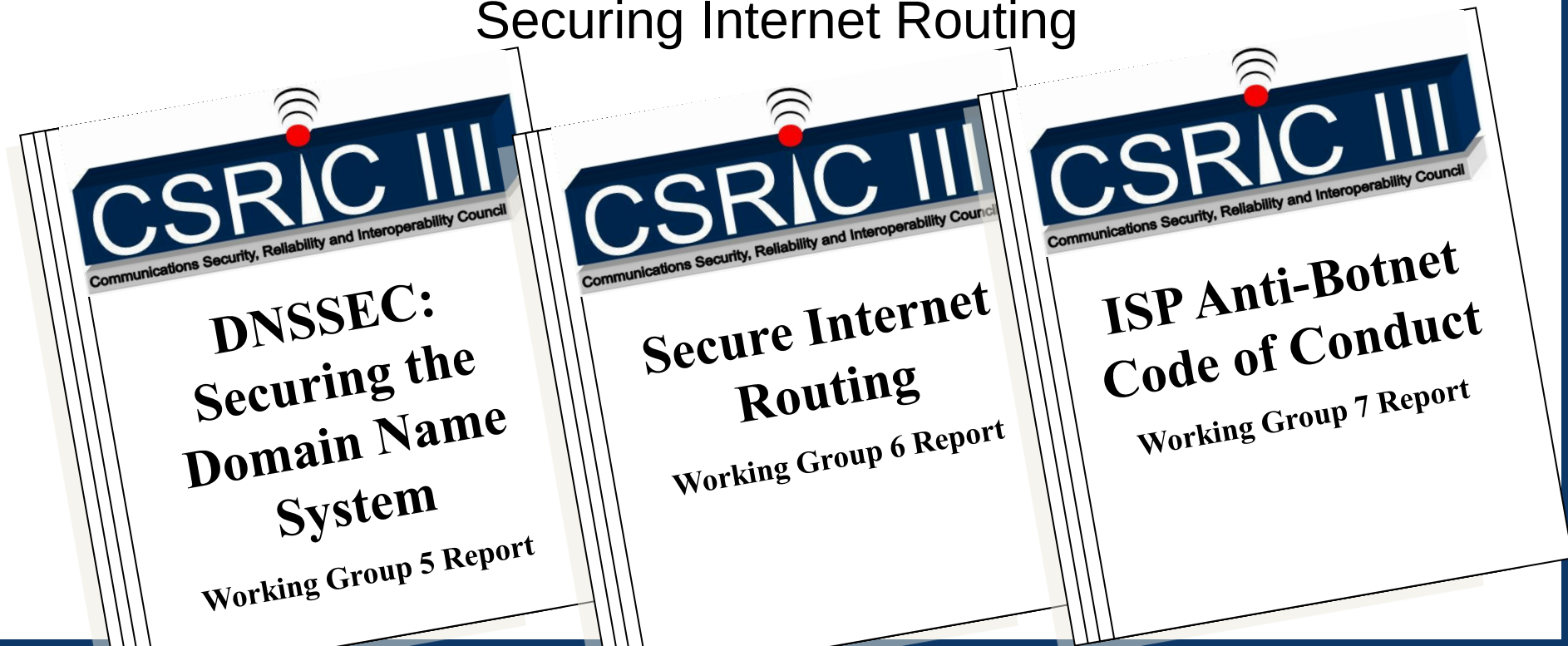
Botnet Attack or
Server Level Attack

Federal Communications Commission

Communications Security, Reliability & Interoperability Council (CSRIC III)

Voluntary Cybersecurity Initiatives for Internet Security Providers

Fighting Botnets, Securing the Domain Name System, & Securing Internet Routing



VENABLE LLP

FCC Communications Security, Reliability & Interoperability Council

The FCC recruited top leaders in cybersecurity to serve on CSRIC III and its working groups, for example:

Mike O'Rierdan
Chairman, MAAWG

Rodney Joffe
CTO - Neustar

Dr. Steve Crocker
CEO Shikuro &
Chair of ICANN

Danny McPherson
CSO - Verisign

Ed Amoroso
CISO – AT&T

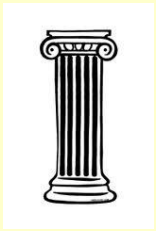
Prof. Jen Rexford
Princeton University

Alan Paller
Research Director
SANS Institute

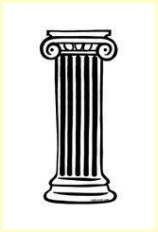
Rod Rasmussen
CTO – Internet Identity

Barry Greene
President – Internet
Systems Consortium

Executive Order 13636: Cybersecurity



Information Sharing: streamline the government's sharing of crucial information (volume, quality, speed) - 120 days



Privacy: Agencies must use Fair Information Practice Principles, DHS assesses and consults with the Privacy and Civil Liberties Oversight Board (PCOB)

Michael Daniel
White House Cyber Coordinator

Standards: NIST shall lead development of voluntary Cybersecurity Framework of standards, methods, procedures for critical infrastructure owners and operators

Three Pillars of EO 13636

Cybersecurity Framework & Process

- Not performance standards per se: methods, best practices
- Consultative and participatory: NIST convenes, stakeholders decide
- Sector Coordinating Councils play big role
- 240 days to draft framework
- 1 year to publish final Cyber Framework
- 120 days DHS/DoC/Treasury recommend incentives to adopt framework
- 120 days DoD/GSA recommend incorporating security standards into acquisition/contracts
- 150 days DHS identifies critical infrastructure at “greatest risk” (where cyber incident could have catastrophic regional or national effects)

Dr. Pat Gallagher
Under Secretary of Commerce
Director of NIST

VENABLE LLP

Cyber Framework Implications

- Government relies on the private sector for the input
- Voluntary, self-governed process and consensus-based
- Government will then set “performance goals”
- Companies will participate to certify that they are compliant
- So, voluntary, but incentives and comparisons may apply
- Defense and other Federal Government contracts: will this set the market?
- Liability if your company does not meet the voluntary standard?
- Will the practical effect be de facto cybersecurity standards
- ✓ Lesson: participate in the process, monitor what is happening

If you don’t have a seat at the table, you may be on the menu

Legislation: CISPA 2013

Cyber Intelligence Sharing and Protection Act of 2013

- House passed CISPA on April 18, 2013 (218-127)
- Bi-partisan effort of House Intelligence Committee Rep. Rogers, Rep. Ruppersberger (but chances in the Senate?)
- CISPA authorizes DNI to share cyber threat intelligence with 'certified entities' or persons with security clearances
- CISPA also authorizes sharing of cyber threat information with the federal government and sets up some protections and privacy safeguards
- But privacy advocates are up in arms and claim that CISPA allows warrantless searches of information from personal email and Internet providers
- Facebook and Microsoft had supported but now do not support CISPA
- White House veto threatened (privacy and 4th Amendment concerns)

Rep. Mike Rogers, R-Mi

Rep. Dutch Ruppersberger, D-Md

Cyber Policy Needs

- Legislation: Incentives, limitation of liability for information-sharing, cyber firehouse (government support during attacks when called)
- New organs of government
- Reconciliation of existing authorities and targeted expansion of new authorities (recognizing that the first line of cyber defense is in the commercial sector)
- National Critical Infrastructure Cyber Exercise Capability
- National Cyber Doctrine

Doctrine: (n.) a body of principles that is advocated and taught

Questions

Backup slides follow

Jamie Barnett
jbarnett@venable.com
(202) 344-4695