NSA: Devil or Security Agency for Democracy?

Virgil Gligor
Carnegie Mellon University
Pittsburgh, PA 15213

Swiss Cyber Risk Research Conference
Swiss Tech Convention Center - EPFL
Lausanne, Switzerland
May 20, 2016

Full Disclosure

1. I've had:
   - *no NSA funding*, research or otherwise, direct or indirect, and
   - *very few contacts* with the NSA leadership (e.g., Dir/DDirNSA, CTO) during the past 7 years

   & *neither* are planned for the near future …

2. I've used *only public information*
   - *no* security clearance, *no* leaks ☺

3. I don't *speak for* any organization with whom I've been affiliated directly or indirectly

   & *all* opinions expressed and errors are *my own*.

NSA: Devil or Security Agency for Democracy?

Answer: Both

. . . for some (e.g., non-religious) definitions of Devil and Democracy

Outline

- what does a cyber-security Devil do & how does s/he do it?
  - Ex: establishing persistent presence in a network– ***not NSA*** specific

- 3 dilemmas for an interconnected world

- possible solutions: The ***NSA*** example

Devil (in cyber-security): an Adversary

establishes *persistent presence* in a Defender's network, by exploiting

- *cost & inconvenience* of tailored security & niche systems
- *fundamental insecurity* of commodity systems & networks
- *frailty of human nature*; e.g., buy, bribe, and blackmail (B3) methods

Devil (in cyber-security): an Adversary

establishes *persistent presence* in a Defender's network, by exploiting

- *cost & inconvenience* of tailored security & niche systems
- *fundamental insecurity* of commodity systems & networks
- *frailty of human nature*; e.g., buy, bribe, and blackmail (B3) methods

Democracy (e.g., in a Western sense): a political system where citizens

- choose/replace government by elections; no revolutions, coups d'etat
- participate in political & civic life => their rights must be protected
- rely on the rule of law; i.e., the law applies equally to all

=> public accountability of government

Devil (in cyber-security): an Adversary

establishes *persistent presence* in a Defender's network, by exploiting

- *cost & inconvenience* of tailored security & niche systems
- *fundamental insecurity* of commodity systems & networks
- *frailty of human nature*; e.g., buy, bribe, and blackmail (B3) methods

Democracy (e.g., in a Western sense): a political system where citizens

- choose/replace government by elections; no revolutions, coups d'etat
- participate in political & civic life => their rights must be protected
- rely on the rule of law; i.e., the law applies equally to all

=> public accountability of government

A Foreign-Intelligence Agency in a Democracy:

=> a Devil for foreign adversaries who threaten its institutions & way of life

Three Dilemmas

1) **for a democracy**: *public* accountability for *foreign-intelligence* operations?

- *no intelligence* to spies, foreign adversaries, terrorists
- *no violations of privacy rights* of citizens under the cloak of secrecy

2) **for a foreign-intelligence agency**: how can one target *foreign adversaries but not citizens* in cyber-space? What is targeting success?

- "*foreignness"* test?
- *intelligence-purpose test*?
- *friend-or-foe* test?

3) **for citizens**: how can we trust that *our own* foreign-intelligence agency *does not spy on us*?
(friends and allies: do we still share same vision of democracy?)

Dilemma 1: Alternate Means of Accountability?

NSA's General Counsel (*Georgetown University Law School*, 27 Feb 2013):

"*There is no perfect substitute for public transparency in a democracy.*"

"…, *we must largely rely on […] alternate means of accountability*"

Dilemma 1: Alternate Means of Accountability?

Executive

DoD (1952) + ODNI (2004)

UnderSec (Intelligence)

AsstSec (oversight)

Gen Counsel

IG (Congress appt)

Gen Counsel

IG (Congress appt)

Civil Liberties Protection Officer

Legislative

House & Senate (1952)

Committees:
Intelligence
Judiciary
Armed Services
Homeland Security, etc.

Judiciary

11 Federal District Court Judges
FISC (Sup. Court. appt.) 1978

Independent

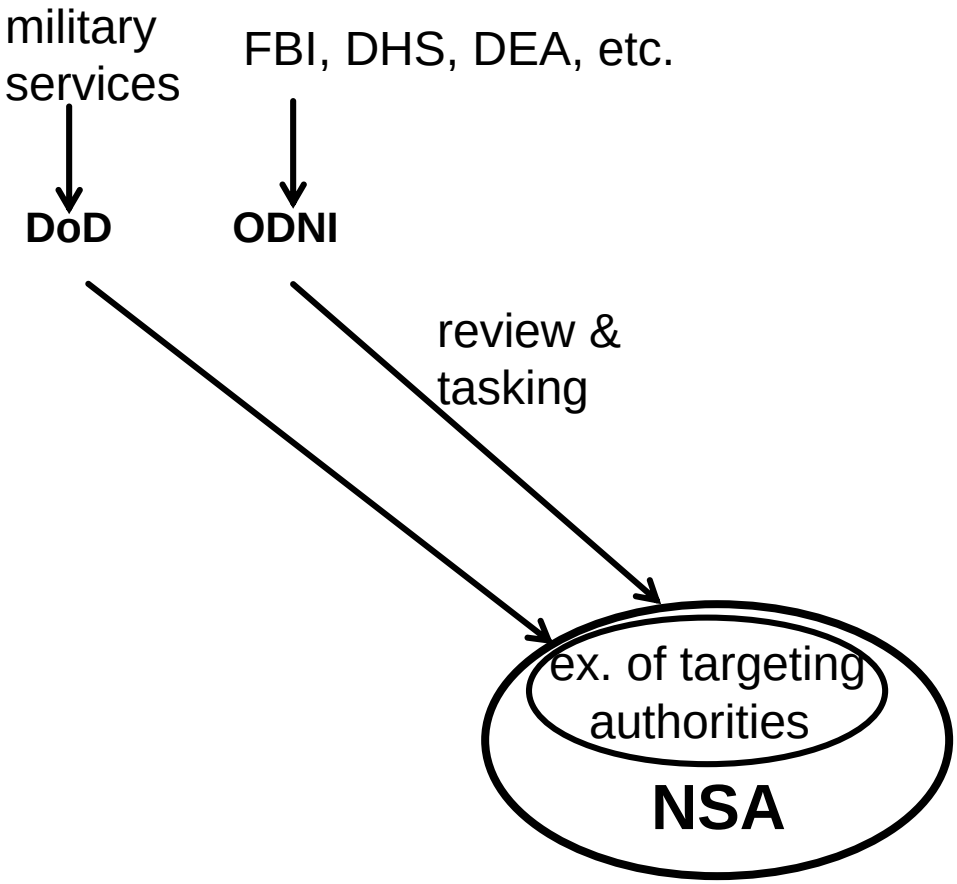
Privacy & Civil Liberties Oversight Board (PCLOB)

2004 – 2006 in the Executive Office?
2007 – 2012 --
2013 – New Independent Board(Jan.)
2014 - Report on PA Section 215
2014 – Report on FISA Section 702
2016 - Assessment Report

Internal

- compliance education, audit, access controls

Dilemma 2: Authorized Targeting?



target*: a *non-US* person *outside US
=> not targeted "intentionally":
- anyone *in US;* US person *outside US (foreigner moves to US -> US person);*
- no wholly-domestic targeting;
- no "reverse targeting" from *outside US;*
- 'minimization procedures"
- *must not violate the 4th Amendment*

purpose: foreign intelligence only

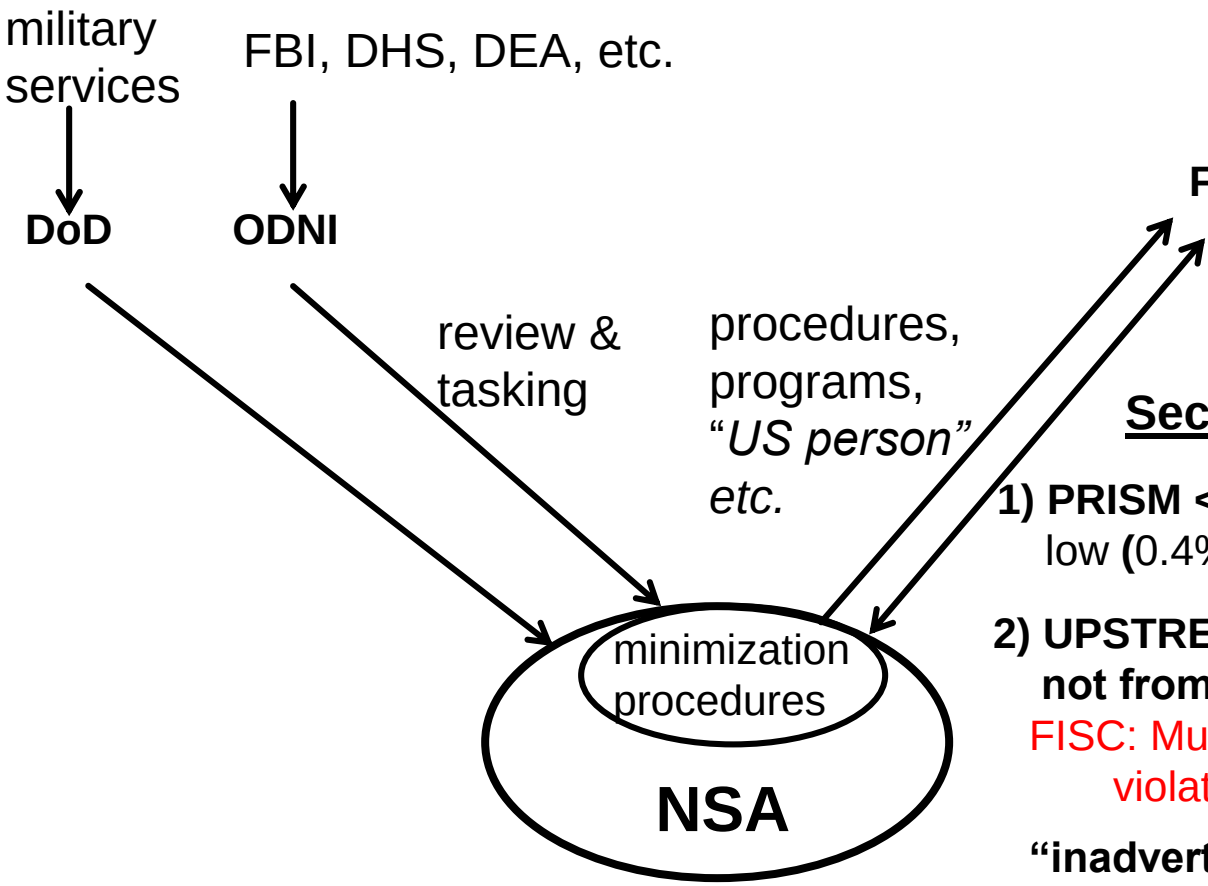
non-US Person targeting?
US ratified 1966 ICCPR (1992)
- Presidential Policy Directive 28 (2014)
  restricted to intelligence acquisition
  same "minimization procedures" as in US

1. Ex. Order 12333
(outside US, 1981)

2. Section 215 of Patriot Act
(inside US, "call records," 2001)

3. Section 702 FISA
(inside US, amended 2008)

Dilemma 2: Correct & Legal Targeting?



FISC – OKed NSA 2012 revisions
ex. 198 US-person authorizations
9,500 US-person queries
89,138 overall targets (2013)

Section 702 FISA

1) PRISM <- specific ISP communication
low (0.4% - 1.5%) error rate in 2013

2) UPSTREAM <- backbone communication
not from specific "to/from/about selector"
FISC: Multi Communication Transactions
violated 4th Amendment (2008 – 2011)

"inadvertent" collection; e.g., via MCT
~7 – 8K US persons, 97 – 140K can't tell
no routine immediate deletion

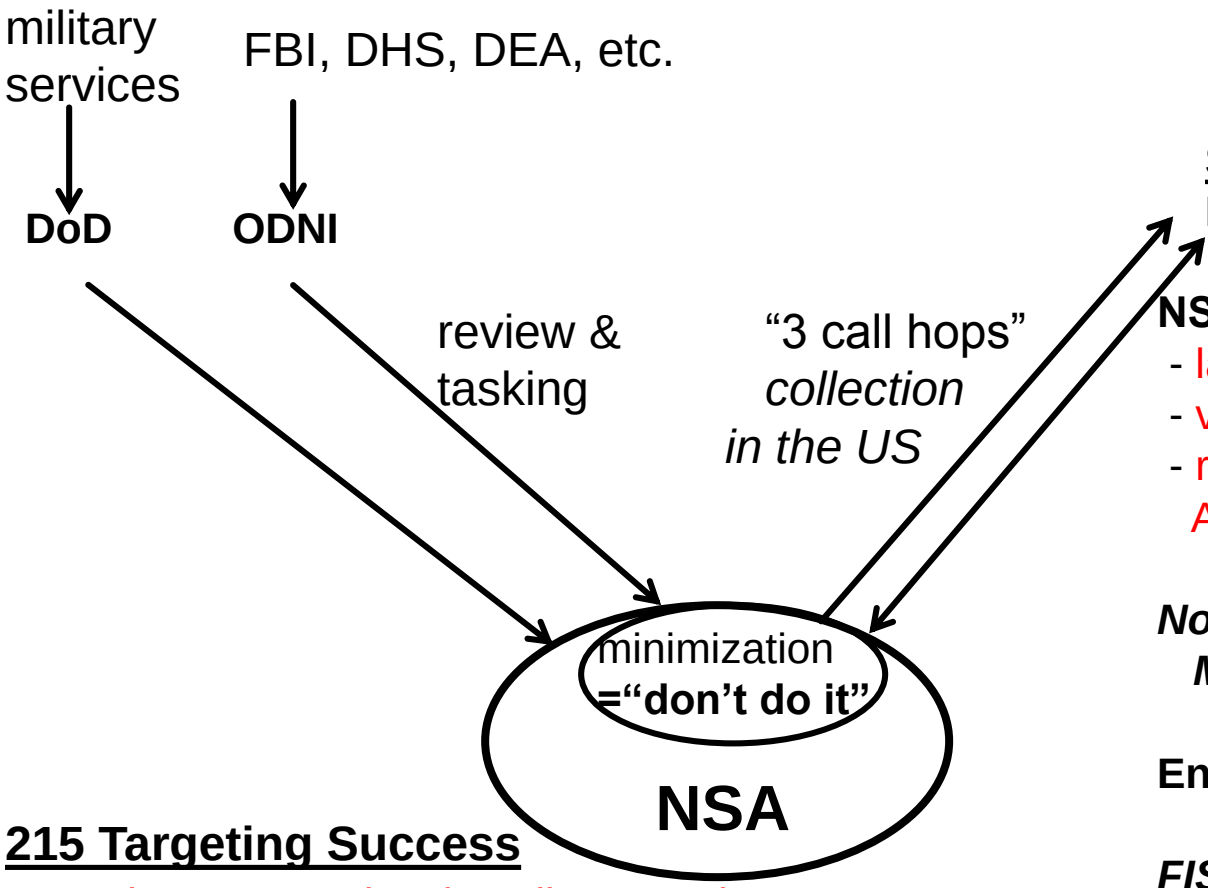
702 FISA Targeting Success

> 100 arrests on terrorism charges
e.g., 15 cases of US plots
40 cases of foreign country plots
weapons proliferation cases, etc.

Executive Order 12333

1) NSA internal audit found & reported
13 willful violations in a decade

Dilemma 2: Correct & Legal Targeting?



Section 215 of Patriot Act
FISC-reviewed every 3 months

NSA's interpretation of Section 215
- lacks legal foundation
- violated ECPA 1986
- raised concerns under 1st & 4th Amendments to the Constitution

No Evidence of Bad Faith or Misconduct by NSA

End bulk call-record collection

FISC lacks
- opposing views & special advocates
- appellate review
- technical & outside legal assistance

Declassification & Stat. Disclosures

215 Targeting Success
- 0 unknown terrorist plots discovered
- 0 terrorist attacks discovered
- 1 arguably unknown terrorist found (no plot)
- additional leads re: contacts of suspects known to FBI
- avoid false positives and saves some FBI resources

Dilemma 3: How do we trust?

Begin with a free press & insider "leaks" ☺

New York Times (Dec. 2005): NSA eavesdrops without warrant
New York Times (Feb. 2006): NSA collected 1.9T call records
- substantial policy changes between 2006 – 2012
- Snowden's revelations (June 2013) accelerated the debate
    - however, piecemeal leaks help create many *false myths* about NSA

Then, insist on independent accountability and legislative action

Independent PCLOB – most recommendations accepted by the US Government
e.g., June 1, 2015 Patriot Act (section 215) expired – no NSA bulk collection

Legislative action; e.g., Email Privacy Act (H.R. 699) – April 27, 2016
e.g., legal warrants needed for
- *email collection* from *service providers*
- obtaining a user's *geo-location data*

Dilemma 3: How do we trust?

"The Americans will always do the right thing … but only after they've exhausted all alternatives."

-- *anonymous 1970 adaptation* of a 1967 Abba Eban quote (misattributed to Winston Churchill)

Finally, debate until you exhaust all alternatives …

e.g., Chilling Effects ... or Only Correlations?

- changes in Internet browsing behavior after Snowden's revelations
  e.g., Pew Research Center (2013), Matthews and Tucker (2015), Jonathon Penney (2016)

- self censorship in browsing re: topics on terrorism?
  OR change of search for "juicier" topics; e.g., Snowden's revelations? OR Both?

- US Federal Judge in rejects Wikimedia "upstream" lawsuit against NSA's (October 2015)
  … no evidence provided of NSA's Internet (i.e., USTREAM) surveillance "at full throttle"

Fact: *91% of all targeted Internet communication is via PRISM*, not *UPSTREAM*

Lessons Learned

1. Total lack of transparency (e.g., "Never Say Anything") has predictable consequences

- leads to *false myths*; e.g., about a dozen about NSA
- eventually *erodes trust in government*

2. When reviewing authorizations, Courts need to hear a Devil's advocate, not just the promoter of the cause (i.e., intelligence agency)

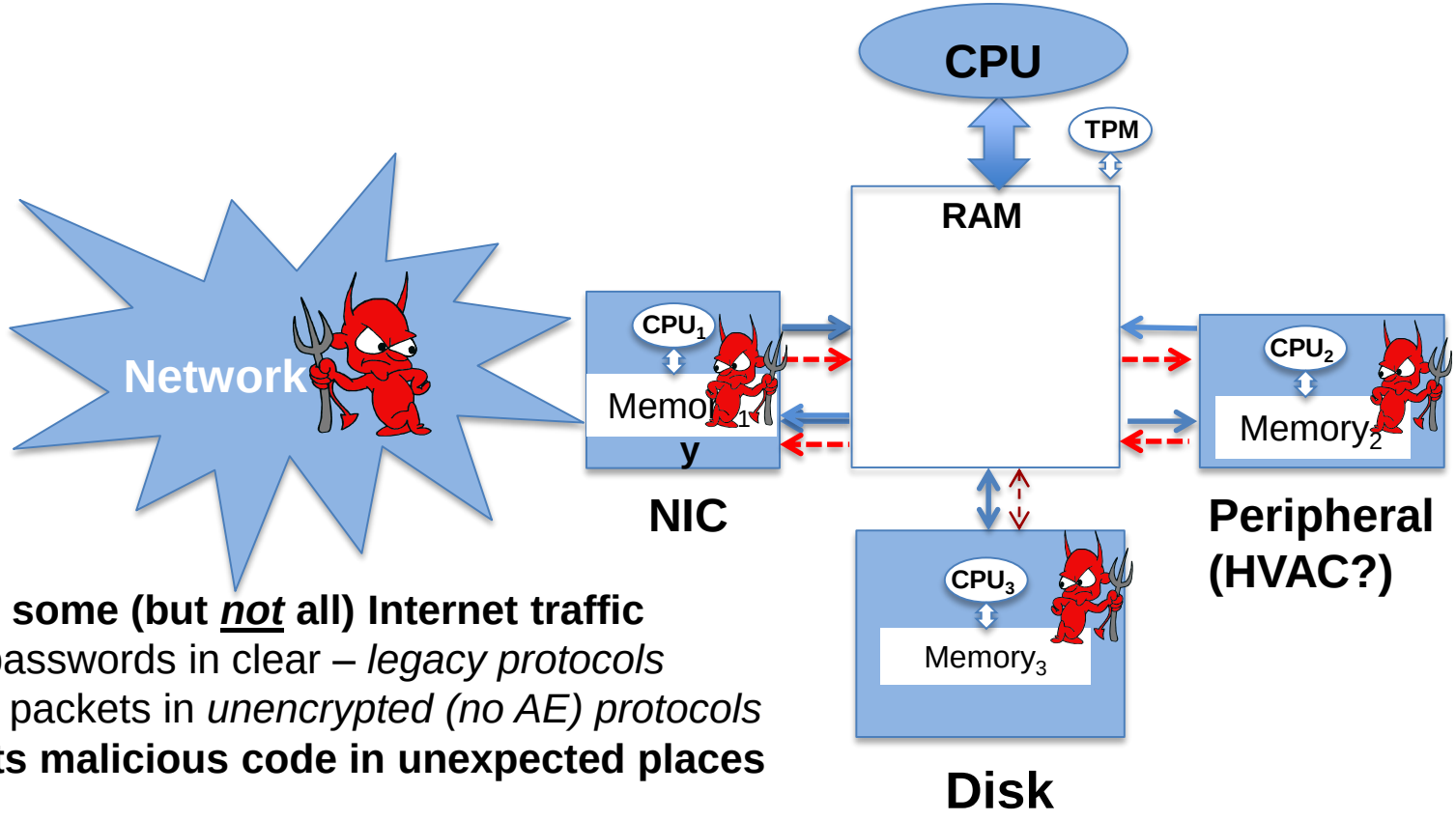
- Courts must avoid the perception of rubber-stamp decisions

3. Law and government policy must keep up with technology

- foreign intelligence authorizations need re-examination more than once in ten years
- no matter how erudite, Courts need help in understanding new technology

Examples:
What does a cyber-security Devil do & how does she do it?

Persistent Presence in a Network – Not an NSA Example

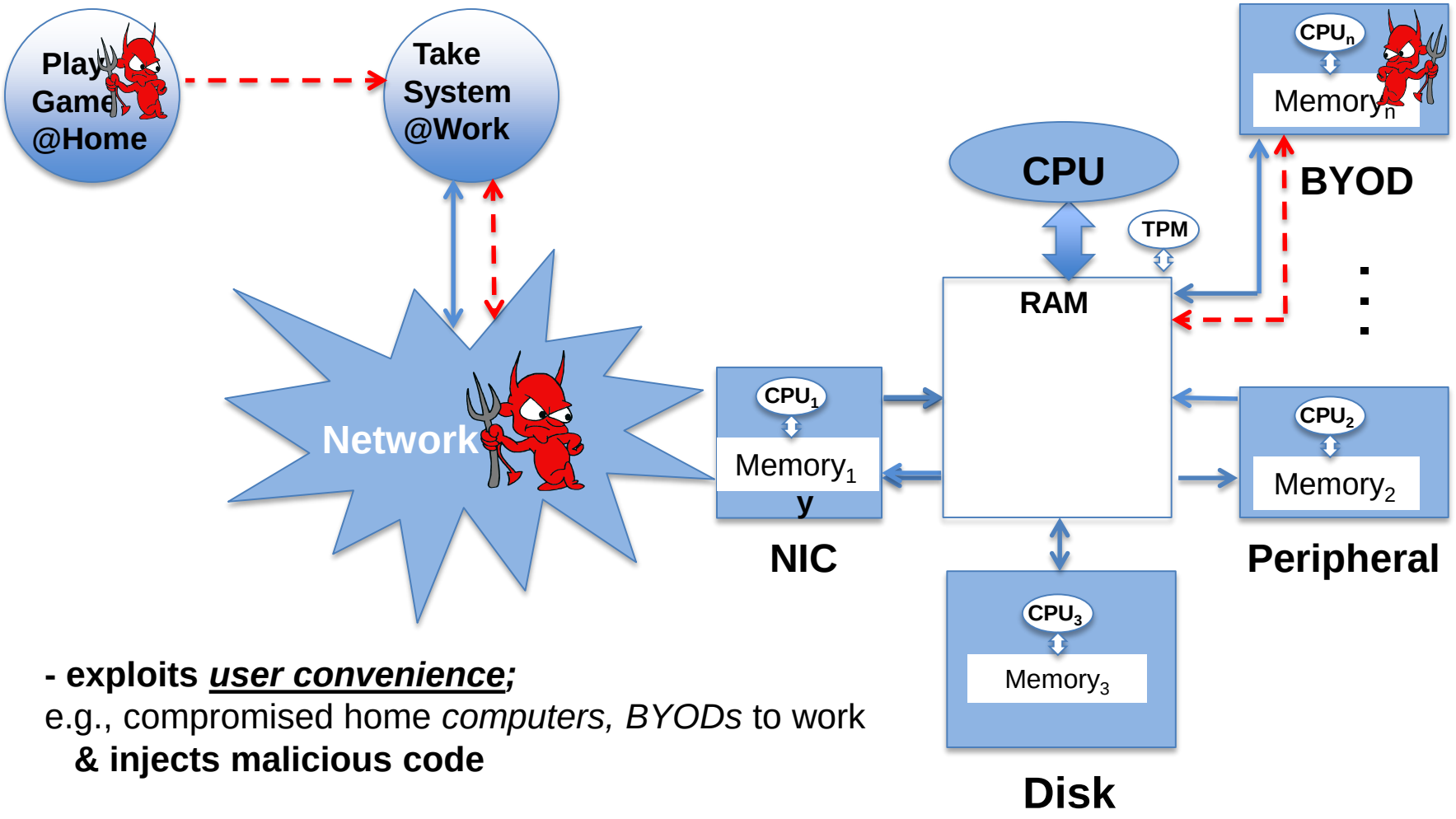


- monitors some (but *not* all) Internet traffic

- finds passwords in clear – *legacy protocols*
- injects packets in *unencrypted (no AE) protocols*

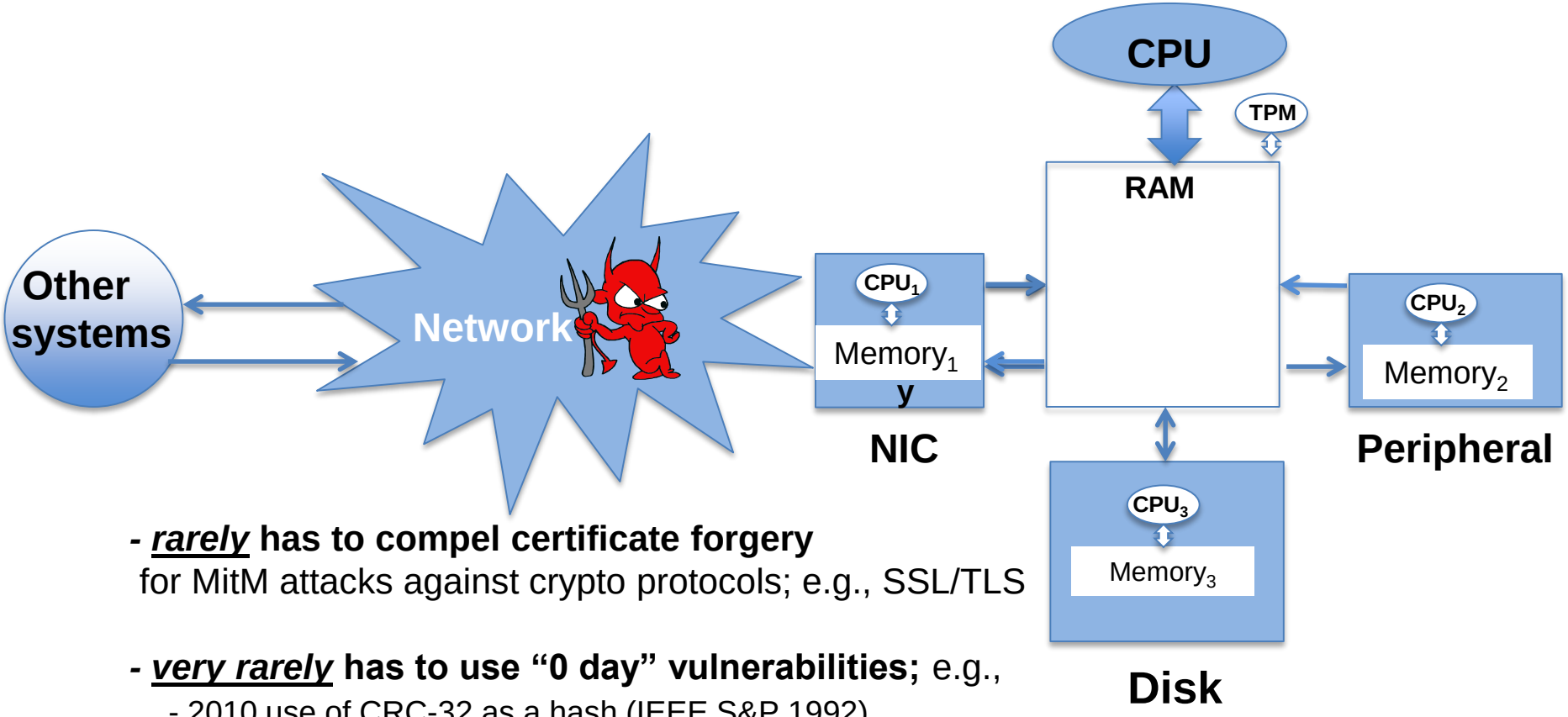
& injects malicious code in unexpected places

Persistent Presence in a Network – Not an NSA Example



- exploits *user convenience;*
e.g., compromised home *computers, BYODs* to work
& injects malicious code

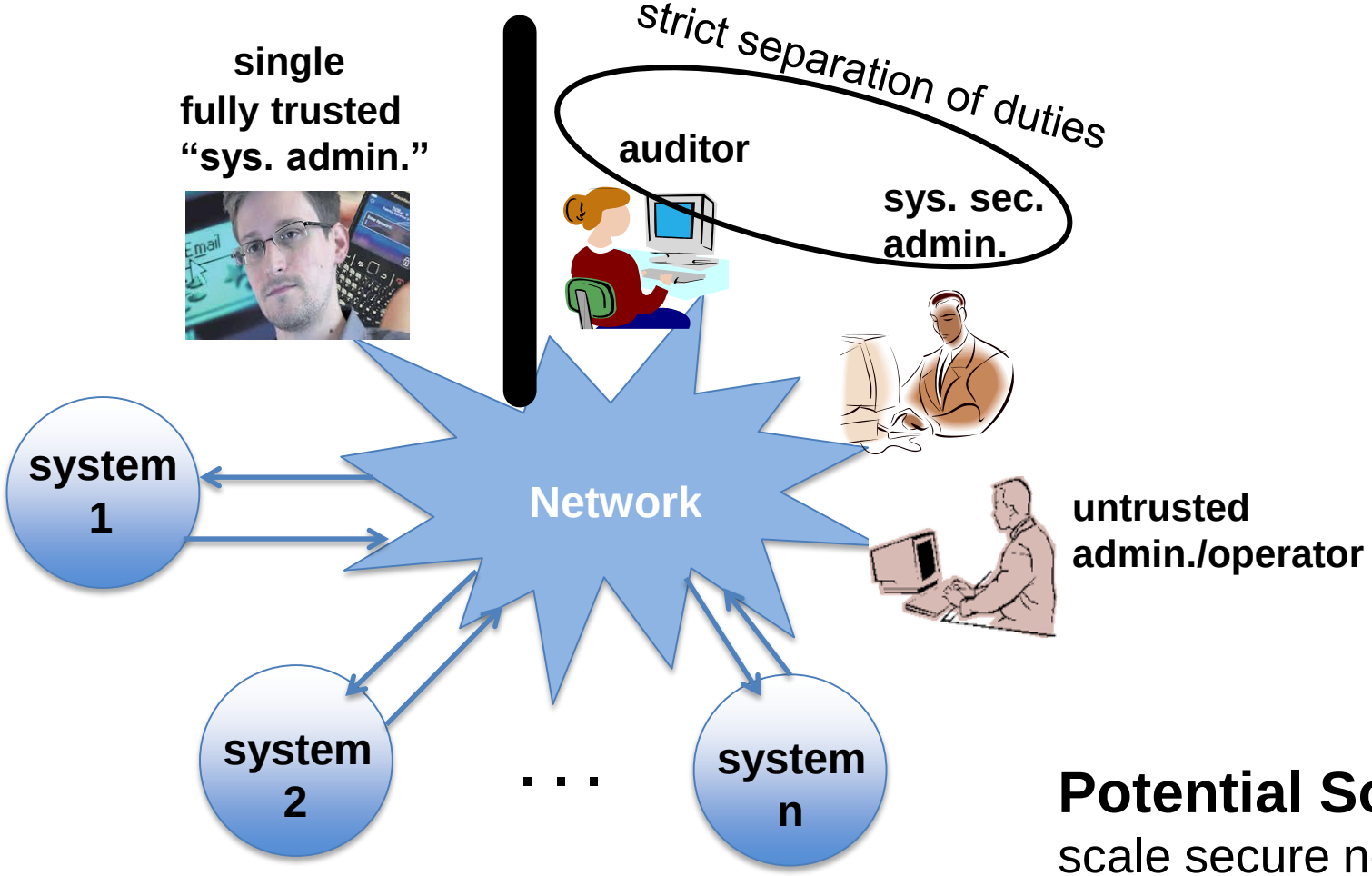
Persistent Presence in a Network – Not an NSA Example



- ***rarely*** **has to compel certificate forgery**
  for MitM attacks against crypto protocols; e.g., SSL/TLS

- ***very rarely*** **has to use "0 day" vulnerabilities;** e.g.,
  - 2010 use of CRC-32 as a hash (IEEE S&P 1992)
  - 2012 MD-5 prefix-collisions (2006 – 2008 TUE - EPFL)

Secure Network Administration: Cost (3x) & Inconvenience



Potential Solution:
scale secure network admin via internal clouds

Fundamental Insecurity of Commodity OSes/Apps

Commodity Software Markets -> **Rapid Innovation** -> **Low/No-Assurance Software**

Characteristics
cost of entry ≈ **0**
regulation ≈ **0**
liability ≈ **0**

Producers
- high productivity; e.g., lots of S/W functions, apps,
- few barriers to using others' code

=> software "**Giants**"

Consumers
- access to lots of functions and apps
- low price

High Assurance/Security
- high latency, opportunity cost
- strict provenance control
  => cannot use others' unverified code)

=> few functions; i.e., **Wimps**

- high cost
  e.g., production & maintenance

Niche Software Markets
e.g., few, small segments of aerospace, defense, nuclear power industries)