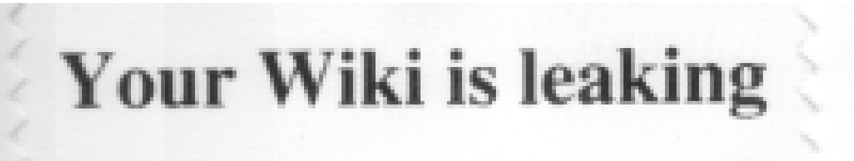
EMAGINED SECURITY

# WikiLeaks, Stuxnet & Other Cyber Weapons - Trust, Treason or Terrorism

**Dr. Eugene Schultz, CISSP, CISM, GSLC**
**Chief Technology Officer**
**Emagined Security**

**Software Security Assurance Summit**
**Huntsville, Alabama**
**March 1, 2011**

# WikiLeaks—a fiasco or treason? (1)



Your Wiki is leaking

# WikiLeaks—a fiasco or treason? (2)

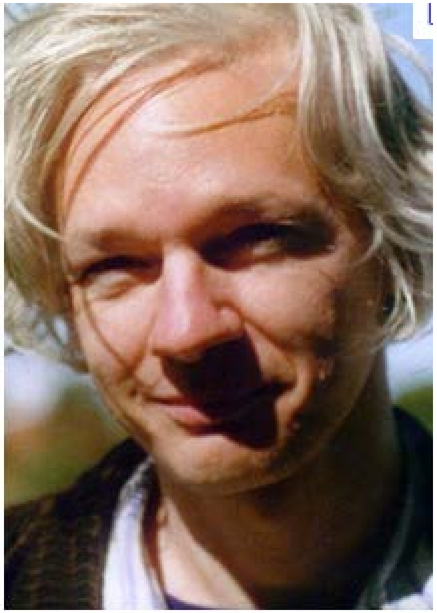
- Charges against Manning include
  - “Transferring classified data onto his personal computer and adding unauthorized software to a classified computer system"
  - “Communicating, transmitting and delivering national defense information to an unauthorized source“
- Such abuse of trust  is difficult to fathom
- Apparent motivation—social justice

Copyright Eugene Schultz 2011 -  All rights reserved

# WikiLeaks—heroic or playing into the hands of bad guys?

EMAGINED SECURITY

- Founded in 2007 to be a safe haven for whistleblowers
- Headed by self-confessed former hacker Julian Assange
- Has posted a disproportionate amount of sensitive and classified information about countries that have freedom of speech



- Activists from "Anonymous" launched denial of service (DoS) attacks against major payment providers
- WikiLeaks' site was also the target of DoS attacks

Copyright 2011 Eugene Schultz - All rights reserved

# WikiLeaks—the "takeaways"

EMAGINED SECURITY

- Manning is in "deep do-do"
- So is Assange
- So is WikiLeaks
- The compromised documents and dispatches for the most part appear to be neither all that valuable nor damaging to the U.S. government
- *This incident shows how information can be turned into a weapon if it falls into the wrong hands*

Copyright 2011 Eugene Schultz - All rights reserved

# The Stuxnet worm (1)

- Spies on and takes control of industrial systems
- Spreads via USB devices
- Remains relatively dormant when it infects Windows systems, but becomes active when it infects Siemens Supervisory Control And Data Acquisition (SCADA) systems
- Subverts an application used in reprogramming these systems, causing damage
- Installs a programmable logic controller (PLC) rootkit that turns motors on and off and changes temperature to cause damage

Copyright 2011 Eugene Schultz - All rights reserved

# The Stuxnet worm (2)

- Attempts to exploit four Windows vulnerabilities (which last August were zero-day vulnerabilities)
  - Vulnerability in how Window manages shortcut files, which execute automatically if copied to a USB drive that the Windows Explorer accesses
  - Vulnerability in the Print Spooler Service that can allow remote execution of unauthorized code if an attacker sends a specially-formed print request to a system with a print spooler interface that is accessible through the Remote Procedure Call (RPC)
  - Two vulnerabilities in which a user who is authorized to run programs on a system or has compromised a system in some other way can become the superuser

Copyright 2011 Eugene Schultz - All rights reserved

# The Stuxnet worm (3)

- Also attempts to exploit a vulnerability in the Server service—requires sending a specially-formed RPC request (MS08-067)
- Has targeted Iranian organizations in particular
- 60 percent of infected systems worldwide have been in Iran

Copyright 2011 Eugene Schultz - All rights reserved

# Stuxnet’s target?

Copyright Eugene Schultz 2011 -  All rights reserved

# Why Stuxnet development was probably well-funded and cooperative

EMAGINED SECURITY

- Sophistication of the code
- Exploited *four* zero-day vulnerabilities
- Almost complete absence of bugs
- Developer(s) had incredibly high level of knowledge concerning how the targeted SCADA systems work

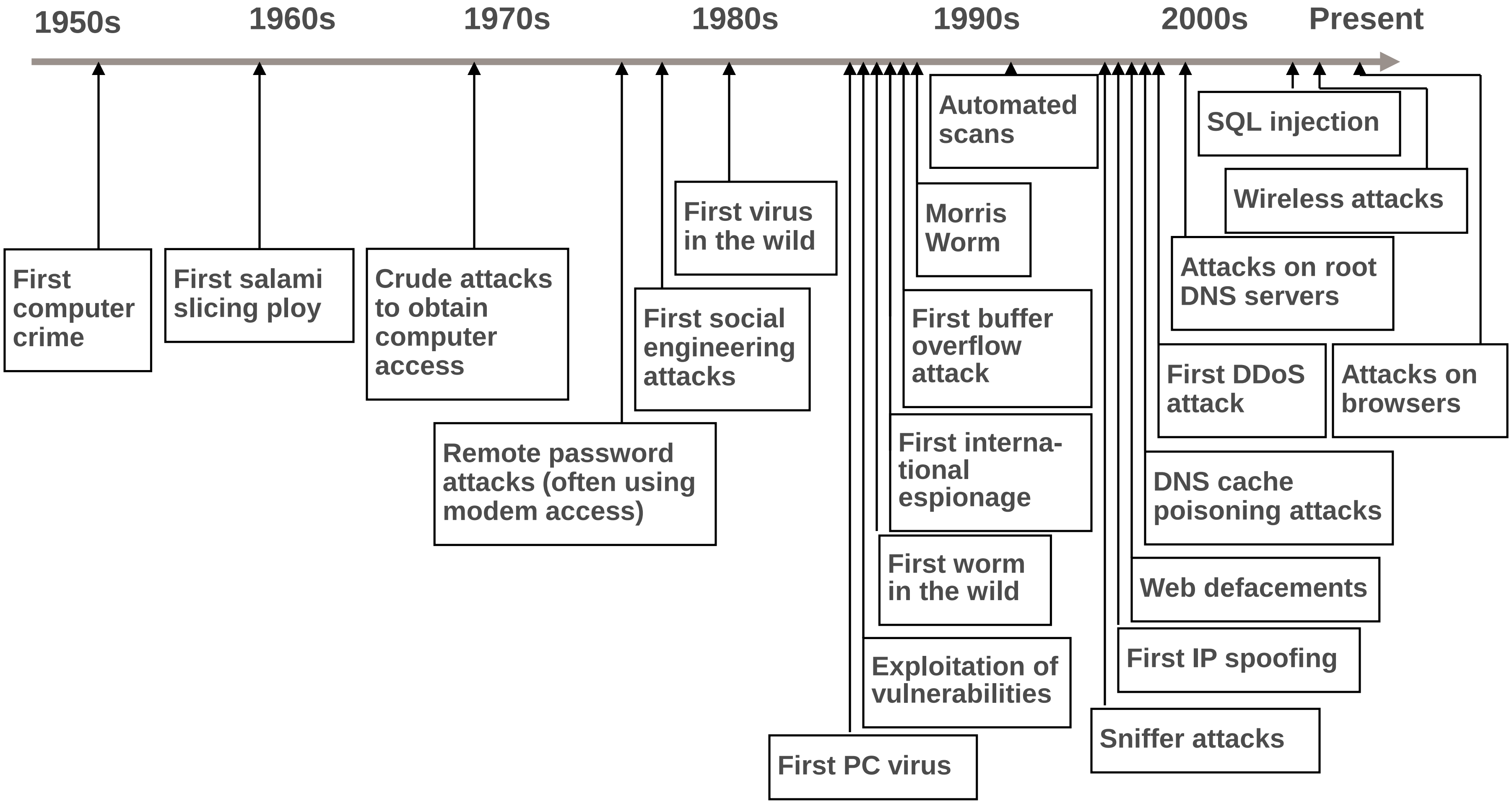
Copyright Eugene Schultz 2011 - All rights reserved

# Stuxnet—the takeaways

- It is now possible to use software to cause serious damage to hardware—in SCADA systems (an almost worst-case scenario)
- Nation states are clearly engaging in cyberespionage
- Worms and other malware are becoming “weapons of mass destruction”
- Infrastructures are becoming the new target

Copyright Eugene Schultz 2011 - All rights reserved

# A threat timeline



1950s

1960s

1970s

1980s

1990s

2000s

Present

First computer crime

First salami slicing ploy

Crude attacks to obtain computer access

Remote password attacks (often using modem access)

First social engineering attacks

First virus in the wild

First PC virus

Exploitation of vulnerabilities

First worm in the wild

First international espionage

First buffer overflow attack

Morris Worm

Automated scans

Sniffer attacks

First IP spoofing

Web defacements

DNS cache poisoning attacks

First DDoS attack

Attacks on root DNS servers

SQL injection

Wireless attacks

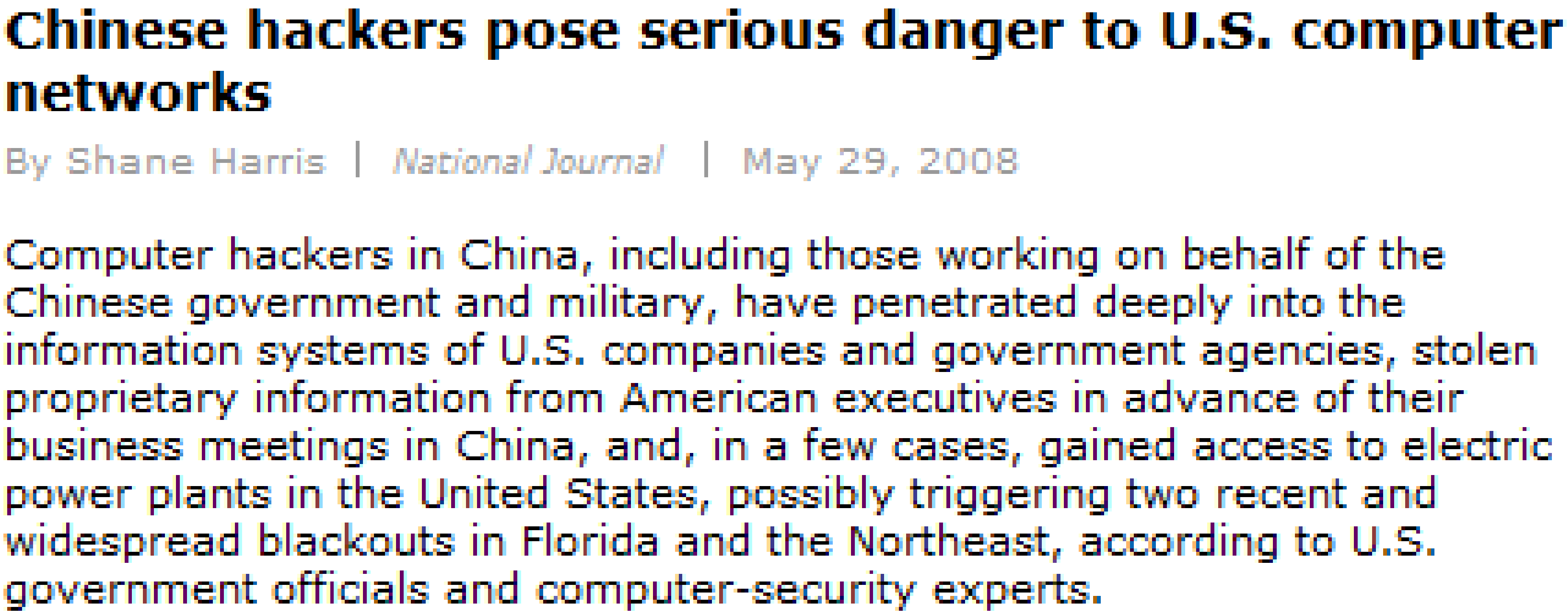
Attacks on browsers

# 2009—a bad year for security

- South Korea and the U.S. targeted in massive DDoS attacks—origin of the attacks was *North Korea's* telecommunications ministry.
- The advent of 64-bit rootkits
- Conficker worm infected possibly as many as 20 million PCs
- Earliest variant of Stuxnet worm was discovered in the wild
- In 2009 the U.S. government admitted that software had been found that could shut down the nation's entire power grid

Copyright Eugene Schultz 2011 - All rights reserved

# The master of cyberweaponry



## Chinese hackers pose serious danger to U.S. computer networks

By Shane Harris | *National Journal* | May 29, 2008

Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast, according to U.S. government officials and computer-security experts.

# There is no end in sight! (1)

- Software vendors keep releasing buggy code
- Attackers keep developing new attack methods
- People, the weakest link, are often the targets
- Malware has become incredibly sophisticated and diverse
- Attacks are very persistent
- Users and organizations fail to embrace and invest in information security

Copyright Eugene Schultz 2011 - All rights reserved

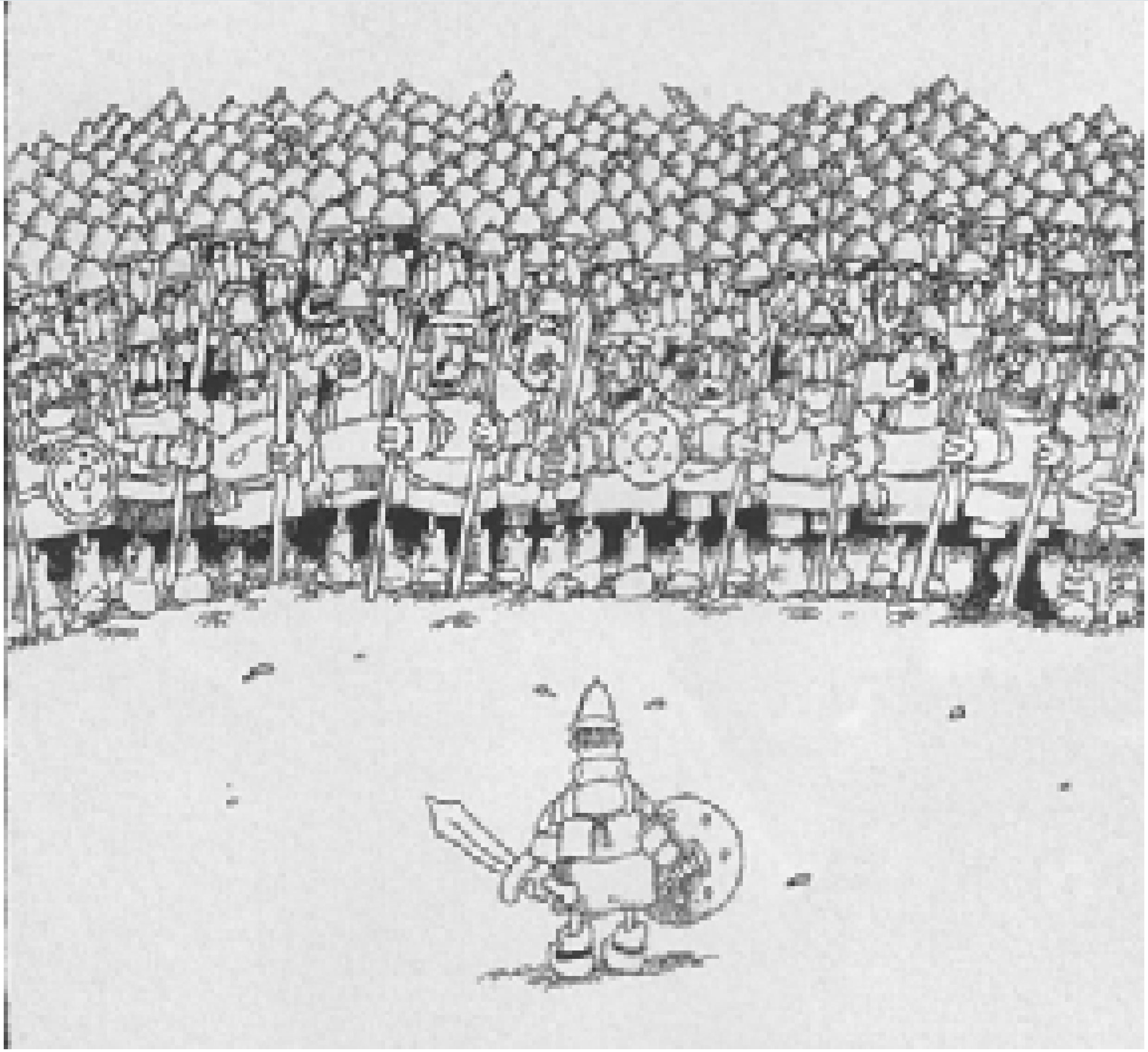
# There is no end in sight! (2)

EMAGINED SECURITY

- Terrorism and use of the Internet are becoming increasingly linked
- Nation states and crime rings provide incredible amounts of money to sponsor attacks and malware development
- We can’t even trust people we are supposed to be able to trust

Copyright Eugene Schultz 2011 - All rights reserved

# Have the threats exceeded our ability to deal with them?

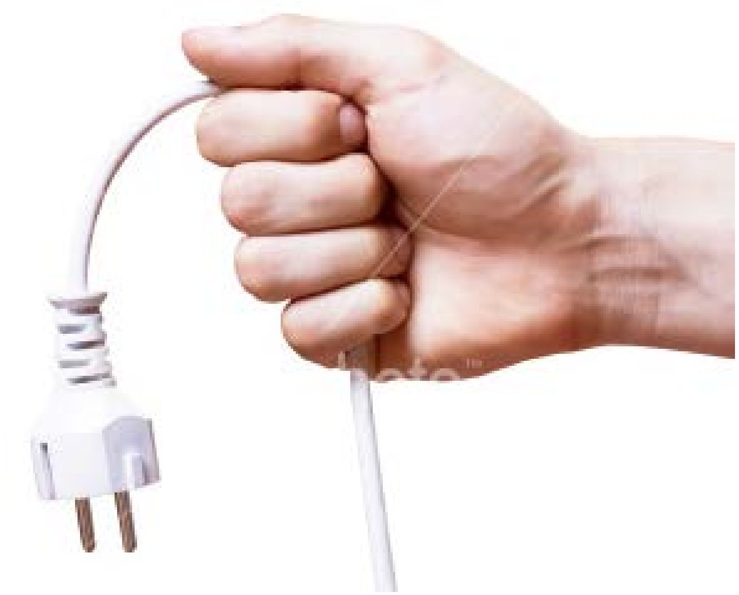


Copyright Eugene Schultz 2011 - All rights reserved

# A frightening thought

EMAGINED SECURITY

*If the Internet can be and is being used as a weapon, why doesn’t someone have the authority to “pull the plug?*



Copyright Eugene Schultz 2011 - All rights reserved