Research Challenges in Tailored Trustworthy Spaces

Dr. Sam Weber

Trustworthy Computing Program, NSF

What is Trustworthy Computing?

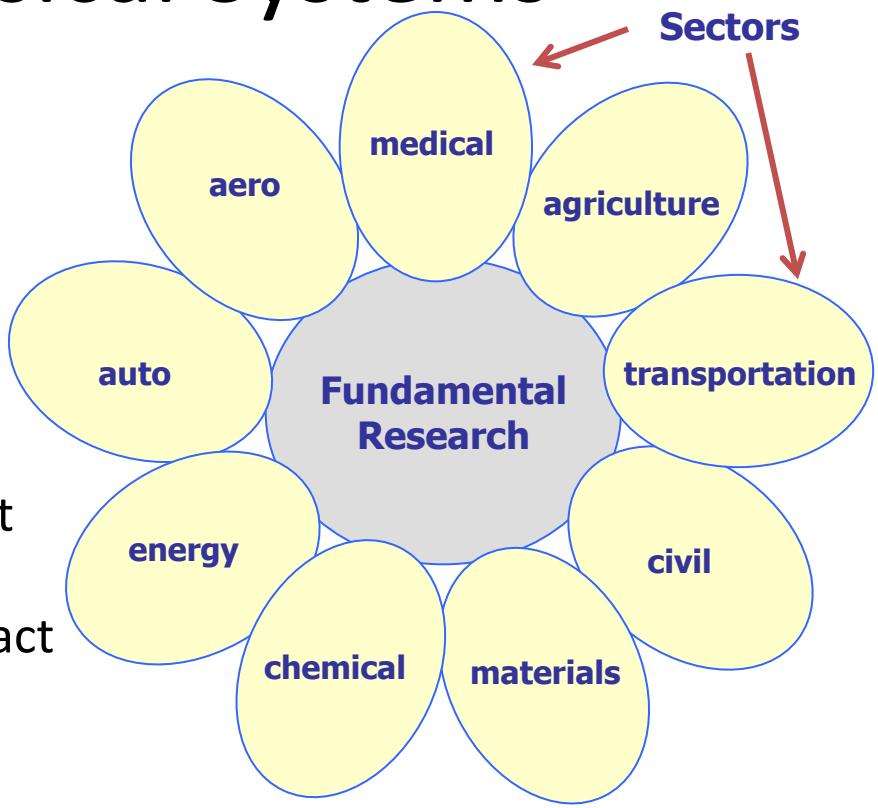
(from FY11 solicitation)

- "Envisions a future pervasive cyber infrastructure that supports a wide range of requirements for trustworthy operation, despite known and future threats and an increasingly complex operating environment. Trustworthy operation requires security, reliability, privacy, and usability. "
- Supports approaches from theoretical to experimental to human centric
- Theories, models, cryptography, algorithms, methods, architectures, languages, tools, systems, and evaluation frameworks
- Studies of tradeoffs among security, privacy, usability
- Methods to assess, reason about, and predict system trustworthiness
- Methods to increase attacker cost, **enable tailored security environments**, and incentivize security deployment, socially responsible behavior, and deter cyber crimes
- Multi-disciplinary work incorporating legal, social, and ethical implications strongly encouraged

- Small / Medium / Large (to $500K / $1.2M / $3M) awards totaling $55M

Cyber-Physical Systems

- Cyber-Physical Systems
  - deeply integrate **computation, communication, and control** into **physical** systems
  - exploit pervasive, networked computation, sensing, and control
- "CPS will transform how we interact with the physical world just like the Internet transformed how we interact with one another."
- **CPS Solicitation (NSF 11-516)**
  - Abstracting from sectors to more general principles
  - Apply these to problems in new sectors



•CPS Summit Website: http://varma.ece.cmu.edu/summit/index.html

Trustworthy Cyber Infrastructure for the Power Grid

(TCIPG, University-Led Collaboration)

Vision: *Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure*

Recent Papers

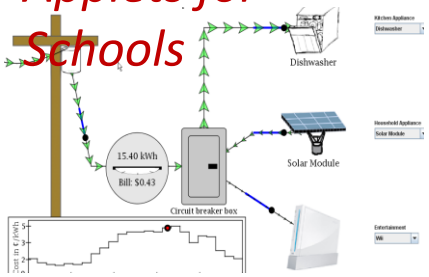
Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

Katherine M. Rogers, *Student Member, IEEE*, Ray Klump, *Member, IEEE*, Himanshu Khurana, *Senior Member, IEEE*, Thomas J. Overbye, *Fellow, IEEE*

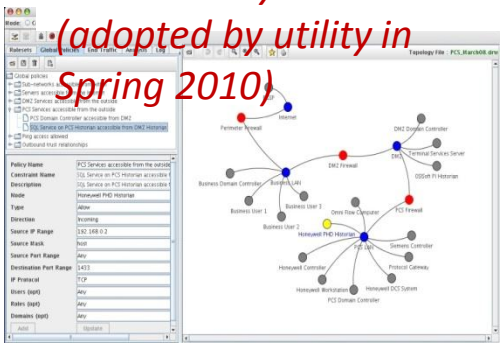
Building Security In

Smart-Grid Security Issues

Applets for Schools



TCIPG NetAPT Network Access Policy Tool (adopted by utility in Spring 2010)



Funding started with NSF, transferred to DOE and DHS

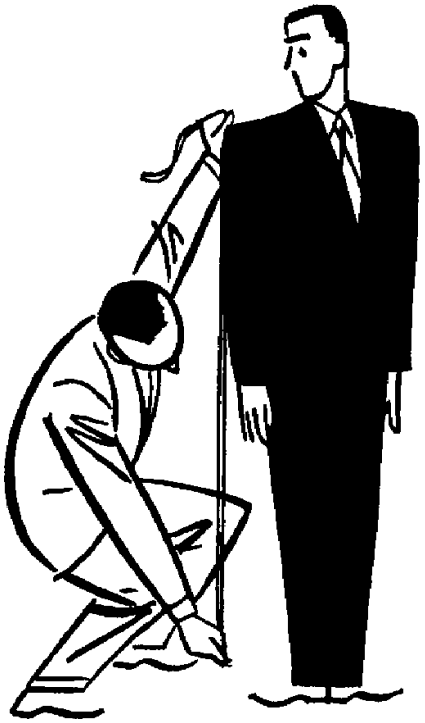
Facilities

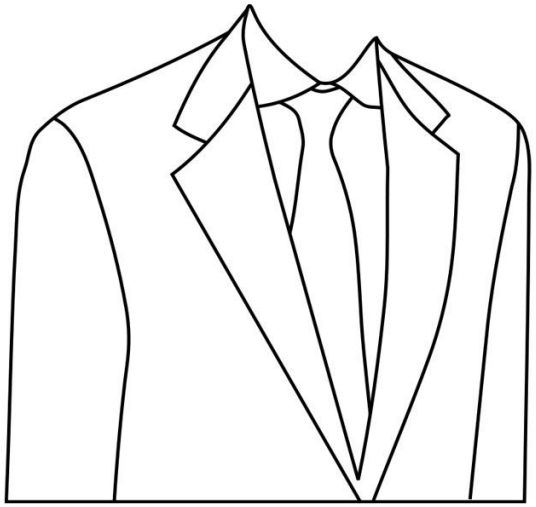
Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

Game-changing R&D Needed to Make *Survivable* Systems a Reality

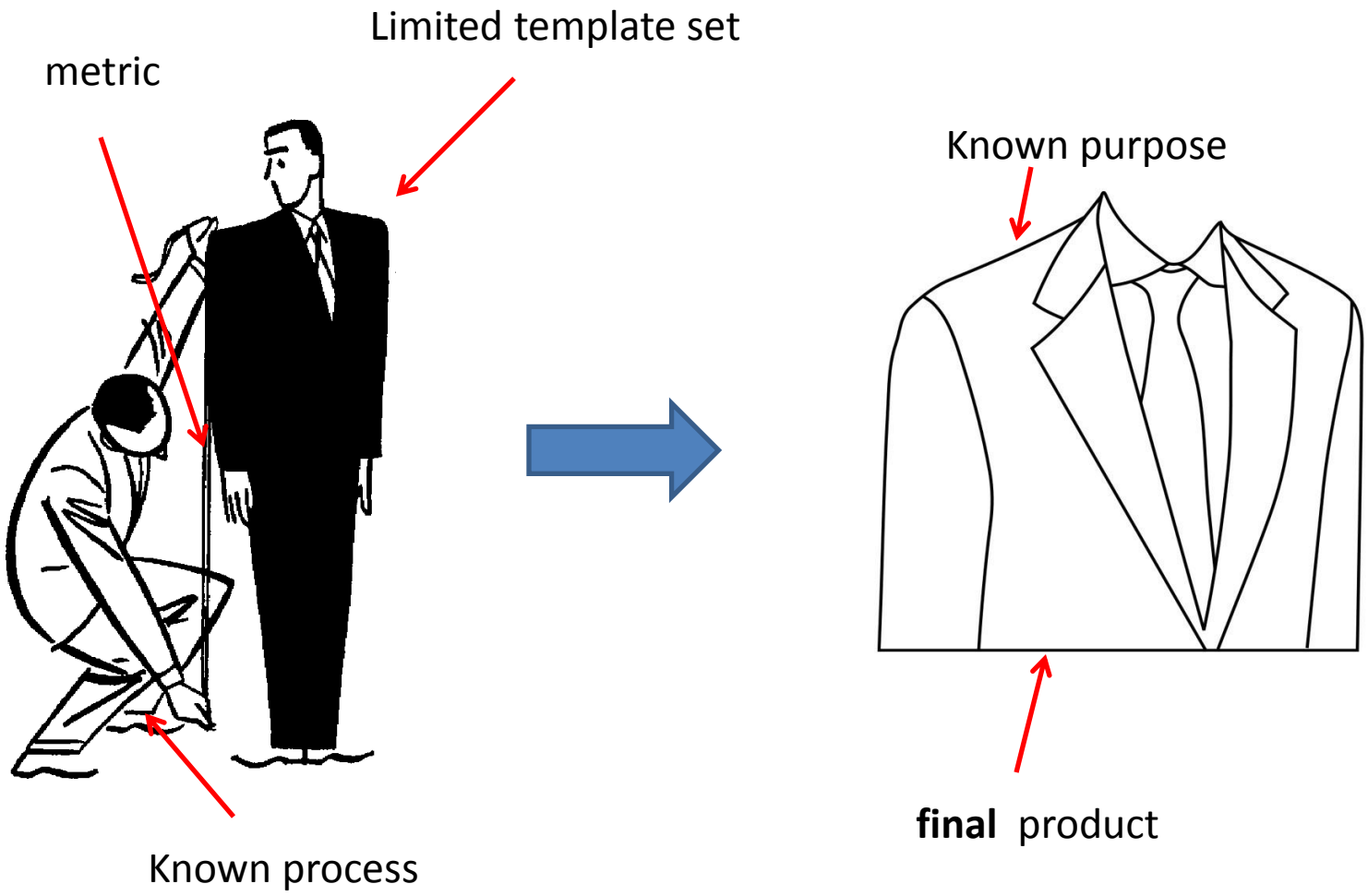
University of Illinois • Dartmouth College University of California at Davis• Washington State University

Tailored Trustworthy Spaces





Tailored Trustworthy Spaces

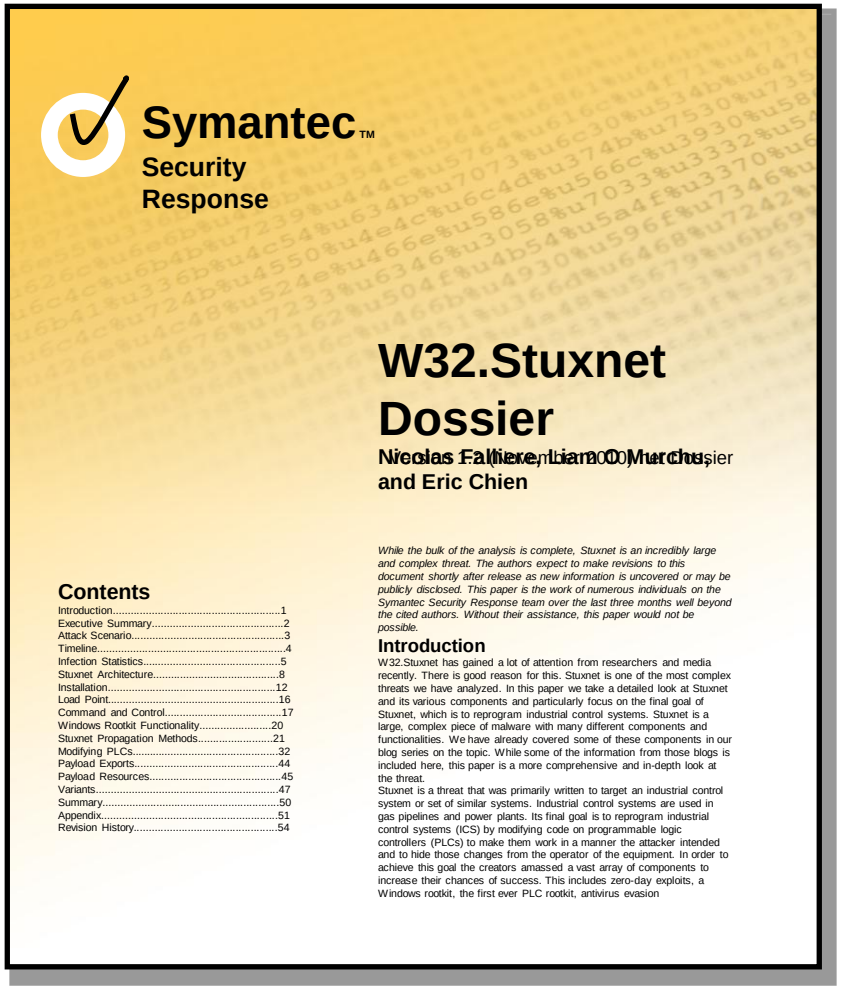


Metrics?

- What are principles, resources? Does "ownership" exist?
  - Eg. health care records
  - Eg. pacemakers
  - Eg. privacy implications of power usage
  - Eg. does anyone know actual policy?

Stuxnet

- Preliminary version seen June 2009
- Final version June 2010
- Reverse engineered, exposing sophisticated attack on Siemens S7 controllers (presumably of Iranian centrifuges), August – November 2010
- Exploits 4 zero-days, jumps airgap via USB
- Ralph Langner, Langner Communications:
  - “Even though Stuxnet … is not a generic attack, several parts of [it] are generic, and … these are easy to copy.”
  - “Once .. these generic attack techniques are implemented in exploit tools… all bets are off. Mitigation of any of these exploits is very difficult”



Symantec™
Security Response

W32.Stuxnet Dossier

Nicolas Falliere, Liam O Murchu, and Eric Chien

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.

Contents

Introduction....1
Executive Summary....2
Attack Scenario....3
Timeline....4
Infection Statistics....5
Stuxnet Architecture....8
Installation....12
Load Point....16
Command and Control....17
Windows Rootkit Functionality....20
Stuxnet Propagation Methods....21
Modifying PLCs....32
Payload Exports....44
Payload Resources....45
Variants....47
Summary....50
Appendix....51
Revision History....54

Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our blog series on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion

http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html?page=full

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?ref=stuxnet

Meaning of “Trustworthy”?

- Realistic threat models?
  - Car tuners, thieves, blackmailers, terrorists
- Security vs safety
- How to respond to threat?
  - Nuclear power plant not like airplane or car

Tailored System?

- Systems continually in flux
  - How does new state compare to old? Have assumptions been violated?
- Systems involve humans
  - “Nudging users towards privacy” (Acquisti et al)
  - Implications of incentives?
- Supply chain variations

“Fabric”

- Secure control systems
  - See TRUST center
  - Resonance effects
- How to sandbox code with different environmental assumptions?

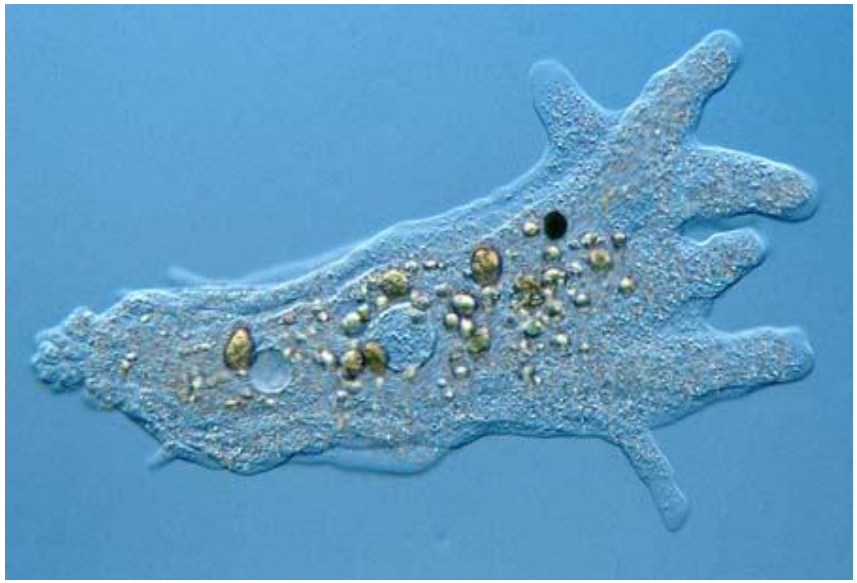
Summary

- Tailoring for amoebas
- See NSF active awards:

www.nsf.gov/awardsearch

Many search options available

Trustworthy Computing = Prog. Element 7795

Cyber-Physical Systems = Prog. Element 7918

Results include abstract of award and PI-email