

Almost 20/20 Foresight – A Model for the Use of Malware in Control Systems

Thomas Richard McEvoy

Information Security Group
Department of Mathematics
Royal Holloway, University of London, UK

January 21, 2011

A Scarcely Considered Battleground

- ▶ The term “cyber warfare” is overused and abused
- ▶ Espionage, or propaganda, would be a more accurate description of most computer borne security threats
- ▶ But on process control aka SCADA systems, it is a feasible concept
- ▶ Yet such systems are the least considered and the least well-defended[4]
- ▶ In spite of both their ubiquity - some examples
- ▶ And the potentially large impact of their failure [6]

A Very Public Threat

- ▶ In 2009/10, malware attack discovered against SCADA systems
- ▶ Momentarily focused public attention on the issue
- ▶ Known as “Stuxnet”, it targeted systems belonging to Siemens Ltd
- ▶ Possibly a specific site (in Iran?)
- ▶ Attributed to various parties

Model of an Attack

- ▶ Probably the best technical analysis of the attack is provided by Symantec [11]
- ▶ Not going to go into detail on this, but will refer to it
- ▶ Show a (fairly) accurate model for the attack was developed in last decade by researchers
- ▶ What else was predicted (that hasn't happened yet)?
- ▶ What research is being done to detect and defend against such attacks?

Outline

- ▶ SCADA systems and security problems
- ▶ Outline of the Stuxnet attack and “predicted” features –
 - ▶ Social engineering
 - ▶ Concealment techniques
 - ▶ Hooking
 - ▶ *Signal manipulation*
 - ▶ *Agent-based* (latent, semi-autonomous) control
- ▶ What else?
- ▶ Research problems

What is a SCADA system?

- ▶ SCADA: Supervisory control and data acquisition
- ▶ DCS: Distributed Control System
- ▶ Geographically distributed computer network used to provide oversight of a process control system
- ▶ Indirect control – sets parameters for production, monitor output for quality and safety
- ▶ Actual control carried out by DCS - control loops consisting of control units, sensors and actuators

SCADA System Architecture

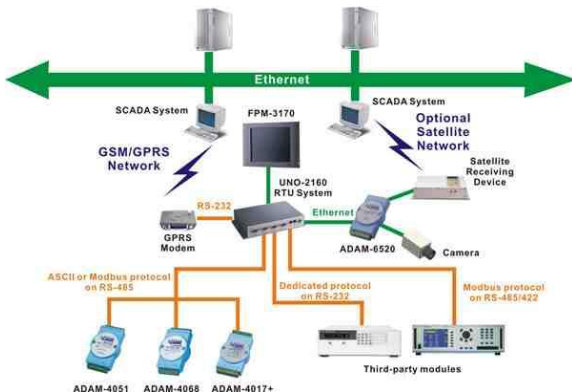


Figure: SCADA System Architecture

Distributed Control Architecture - Control Loop

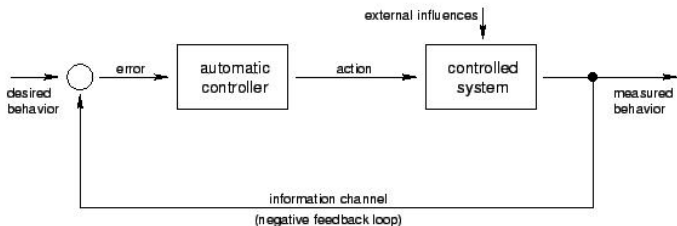


Figure: Simple Control Loop

Example System - Tennessee Eastman

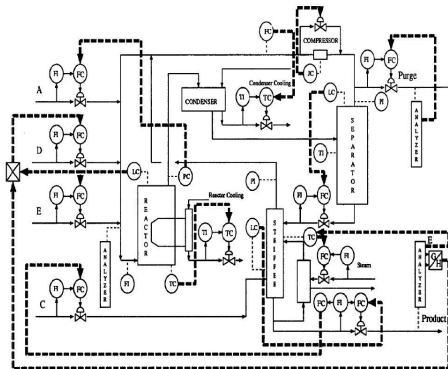


Figure: More Complex System [5]

Security in SCADA Systems

- ▶ Previously isolated, esoteric ('eccentric') systems
- ▶ Security concerns were restricted to physical, procedural and personnel dimensions
- ▶ Nowadays, such systems can be characterized as COTS, fully internetworked and fully programmable
- ▶ Changes have advantages, but expose the system to attack
- ▶ Systems life expectancy increases exposure to dynamically evolving threats
- ▶ Industry does not have the cultural or organisational experience to evolve
- ▶ Resistant to measures which downgrade performance and/or reliability
- ▶ Cyber threat model shifting to long term goals (APT)

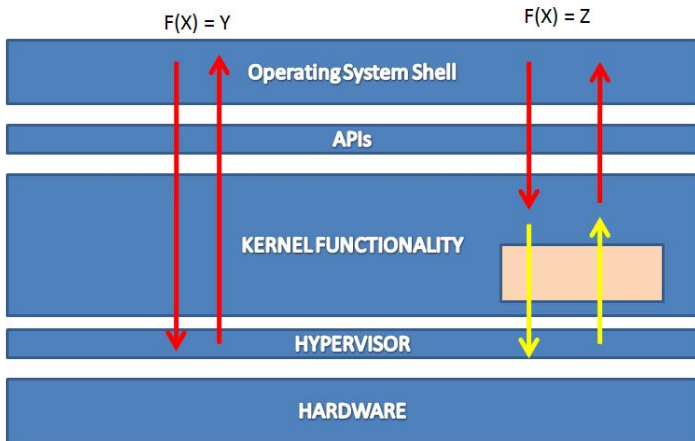
Stuxnet Attack Features

- ▶ Professional nature [3]
- ▶ Social engineering [2]
- ▶ Multiple attack/distribution vectors [13]
- ▶ Avoiding detection by –
 - ▶ Appearing normal [2]
 - ▶ Utilising rootkit techniques [8]

Predicted Features ctd

- ▶ Hooking functionality [1]
- ▶ *Signal manipulation* [10] - cute stuxnet feature!!!
- ▶ *Agent based* attack [9]

Hooking



Signal Manipulation

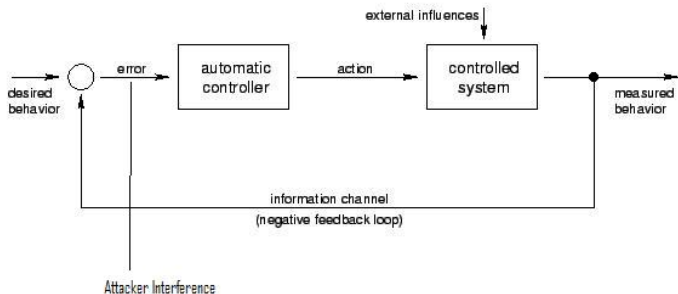


Figure: Attacker Interference in Control Unit

Agent Based Attack[9]

- ▶ In Dolev Yao model, the attacker has full charge of communication
- ▶ In agent based model, the attacker's ability to communicate is limited
- ▶ The attacker can re-write process functionality
- ▶ Subverted processes take on limited decision making and subversion capabilities
- ▶ Model expressed algebraically to permit formal reasoning about "non interference" in channels and processes

Dolev Yao Model

$Adversary := \bar{x}u + x(u) + \tau$

- ▶ Adversary can intercept any message from any concurrent process e.g

$(Alice)\bar{x}a|(Adversary)x(u)|(Bob)x(u)$

- ▶ The adversary can delay/drop/read/manipulate the message by τ

Agent based model

- ▶ Adversary defined as before message handling is prioritised (real time)

$(Alice)\bar{x}a_1 | (Adversary)x(u) | (Bob)x(u)_1$

- ▶ Adversary can rewrite a process $A := A + R + x(m)A'$ such that $A := \bar{x}u_1 + x(u) + \tau + Q$
- ▶ Hence the agent gains an interception and decision making capability (albeit partial due to network segmentation)

Other Attack Vectors

- ▶ Threats may be narrowly perceived as network borne hacking and malware
- ▶ Other entry vectors include –
 - ▶ wireless interception
 - ▶ OOB modem links
 - ▶ physical access
 - ▶ HF radio guns
 - ▶ Private line taps
 - ▶ Hybrid attacks

Other Attack Capabilities

- ▶ Internal denial of service
- ▶ Inter agent communication
- ▶ Use of covert channels
- ▶ Interference in network channels - DOS and manipulation
- ▶ Updating capabilities
- ▶ Interference in other control parameters

Protocol Based Detection

- ▶ Network behavior and protocol usage easier to predict
- ▶ This means that anomaly detection is easier to achieve[4]
- ▶ However, there are limitations
- ▶ Possible to send malicious commands and manipulated signals using legitimate protocols [15]
- ▶ For example, 3 valve problem

Signal Anomaly Detection

- ▶ Another approach is to look for physical signal anomalies [12]
- ▶ But there are dangers in applying such techniques naively [14]
- ▶ For example, let A and B be two controllers where
$$f(B) = g(f(A))$$
- ▶ If A is “unknown” due to signal manipulation then $f(B)$ can have the “correct” mean and variance, but not be causally consistent - not enough to use correlation, regression or even PCA
- ▶ Estimation techniques (e.g. particle filters) needed to predict $(f(B)|f(A))$ and detect anomalies
- ▶ There is also a paucity of models and data for non linear systems [7]

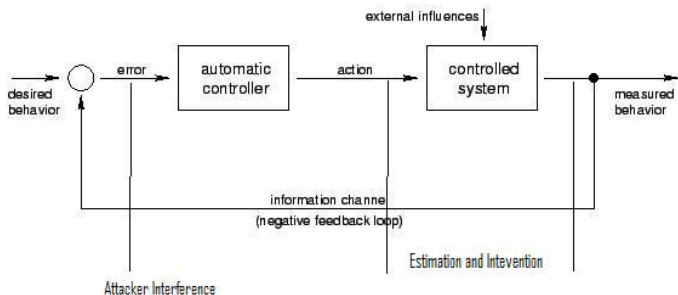
Hybrid State Estimation in Non Linear Systems

- ▶ Challenge: to combine physical and computational state estimation
- ▶ Various approaches - both using formal models and simulations
- ▶ Requires both a realistic control problem with variations in the control approach and non linearity
- ▶ And an accompanying system architecture model which enables us to reason about the reliability of processes and communications
- ▶ Our proposed approach makes use of process algebraic structures
- ▶ Formal model incorporating state estimation and reasoning over channel reliability

The Goose Which Lays the Golden Egg...

- ▶ Detection is only the starting place
- ▶ Prevention is good when it happens
- ▶ The problem is that recovery is not always possible
- ▶ You can't reboot an industrial process
- ▶ So the ultimate goal is *dynamic* intervention

Dynamic Intervention



Summary

- ▶ Cyber warfare is meaningful when applied to SCADA systems
- ▶ Ability to undermine the critical infrastructure of a nation
- ▶ Or cause major impacts similar in effect to terrorist attacks
- ▶ SCADA systems not well defended due to history and
- ▶ Have characteristics which make them hard to defend
- ▶ Stuxnet was an example of a (almost) fully predictable attack; explains some criticisms(!)
- ▶ There will be more
- ▶ Research has concentrated on both protocol and signal anomaly detection but with limited results
- ▶ Future research will need to take on the challenge of hybrid state estimation and dynamic intervention

Questions



Arati Baliga, Pandurang Kamat, and Liviu Iftode.

Lurking in the Shadows: Identifying Systemic Threats to Kernel Data.

In Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P 2007), pages 246–251, Piscataway, NJ, USA, May 2007. IEEE Press.



K. Borders, Xin Zhao, and A. Prakash.

Siren: catching evasive malware.

In Security and Privacy, 2006 IEEE Symposium on, pages 6 pp. –85, May 2006.



Tony Bradley, Anton Chuvakin, Anatoly Elberg, and Brian J. Koerner.

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance.

Syngress Publishing, 2007.



M. P. Coutinho, G. Lambert-Torres, L. E. B. da Silva, J. G. B. da Silva, J. C. Neto, E. Bortoni, and H. Lazarek.

Attack and Fault Identification in Electric Power Control Systems: An Approach to Improve the Security.

In *Proceedings of Power Tech 2007*, pages 103–107, Lausanne, Switzerland, July 2007. IEEE Press.



J. J. Downs and E. F. Vogel.

A Plant-wide Industrial Process Control Problem.

Computers & Chemical Engineering, 17(3):245–255, March 1993.



Joe Falco, Keith Stouffer, Albert Wavering, and Frederick Proctor.

It security for industrial control systems.



David Gamez, Simin Nadjm-tehrani, John Bigham, Claudio Balducelli, Kalle Burbeck, and Tobias Chysler.

Safeguarding Critical Infrastructures.

In *DEPENDABLE COMPUTING SYSTEMS: Paradigms, Performance Issues, and Applications*,. Wiley[Imprint], Inc., 2000.



C. Kruegel, W. Robertson, and G. Vigna.

Detecting Kernel-Level Rootkits Through Binary Analysis.

In *ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*, pages 91–100, Washington, DC, USA, December 2004. IEEE Computer Society.



Richard McEvoy and Stephen Wolthusen.

A Formal Adversary Capability Model for SCADA Environments.

Proceedings, CRITIS 2010, 6, 2010.



T.R. McEvoy and S. D. Wolthusen.

Detecting SCADA Sensor Signal Manipulations in Non-linear Chemical Engineering Processes.

In Proceedings of the IFIP TC 11 25th International Information Security Conference, IFIP Advances in Information and Communication Technology, 2010.



Liam O Murchu Nicolas Falliere and Eric Chien.

"w32.stuxnet dossier v1.3", 2010.



Su Sheng, W.L. Chan, K.K. Li, Duan Xianzhong, and Zeng Xiangjun.

Context Information-Based Cyber Security Defense of Protection System.

Power Delivery, IEEE Transactions on, 22(3):1477–1481, July 2007.



A. H. Sung, J. Xu, P. Chavez, and S. Mukkamala.

Static analyzer of vicious executables (save).

Computer Security Applications Conference, Annual, 0:326–334, 2004.



N. Svendsen and S. Wolthusen.

Modeling And Detecting Anomalies In Scada Systems, pages 101–+.

The International Federation for Information Processing, 2009.



J. Verba and M. Milvich.

Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS).

In Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security, pages 469–473, Waltham, MA, USA, May 2008. IEEE Press.