The Need to Consider Both Object Identity and Behavior in Establishing the Trustworthiness of Network Devices within a Smart Grid

[Extended Abstract]

Owen McCusker
Sonalysts, Inc.
215 Parkway N.
Waterford, CT 06333, USA
mccusker@sonalysts.com

Benjamin Gittins
Synaptic Laboratories Limited
PO Box 5, Nadur, Gozo,
NDR-1000
Malta, Europe
cto@pqs.io

Joel Glanfield
Dalhousie U., Computer Sci.
6050 University Ave.
Halifax, NS, B3H 1W5,
CANADA
glanfield@cs.dal.ca

Scott Brunza
Sonalysts, Inc.
215 Parkway N.
Waterford, CT 06333, USA
scottso@sonalysts.com

Dr. Stephen Brooks
Dalhousie U., Computer Sci.
6050 University Ave.
Halifax, NS, B3H 1W5,
CANADA
sbrooks@cs.dal.ca

ABSTRACT

Today's distributed computing environments, like Energy Control Systems, lack a common and adaptive notion of trust and are vulnerable to a wide range of attacks from complex threats. These threats on our control systems are distributed, decentralized, dynamic, and operate over multiple timescales. Threats may also result from structural weaknesses in system designs that permit exploitation by insiders working inside globally trusted service providers. Although approaches such as Trusted Computing are part of the solution, we argue that a layered notion of distributed trust is required to effectively address the end-to-end security needs of these systems.

Categories and Subject Descriptors

D.4.6, K.4.2 [**Security and Protection**]: Network Behavioral Analysis—*aggregated behavioral analysis, behavioral trust, self and non-self*; E.3 [**Data encryption**]: Identity—*distributed trust, redundant trust model*

General Terms

Layered and Distributed Trust, Identity, Behavioral Trust

1. INTRODUCTION

Energy Control Systems (ECS) are pervasive in nature and are comprised of a hierarchy of distributed physical and electronic sensing, monitoring, and control devices operating in a competitive de-regulated environment. These control systems encompass supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and remote components such as remote terminal units (RTU) and programmable logic controllers (PLC) that monitor system data and initiate control activities.

As stated by the NSTB in [2], "Smart Grid design and deployment must take into account the current cyber vulnerabilities in the legacy power grid." A major focus in Smart Grid development is "resistance to attack." This was noted as being difficult to achieve for several reasons: 1) Increased complexity with future communication paths; 2) Ultimate size of system, combined with increased complexity of threats; 3) "The desire to minimize cost tends to take priority over security when threats are not well understood".

The local and national operational capabilities surrounding a Smart Grid are not focused on any one single entity, but instead are an aggregate of multiple entities, including networks, power stations and control systems all providing various levels of communication and control functions.

In order to realize the defense of these complex systems, we encourage a multi-layered approach that consists of: a) hardened software and operating systems, b) trusted hardware, c) trusted tokens, d) distributed decentralized behavioral sensors within application software, hardware and networks, e) a distribute, decentralized identity management (IdM) framework that associates electronic identifiers (and possibly organizational identities) with hardware tokens, and f) a distributed decentralized IdM framework that associates human users with unique tokens. Trusted software and hardware are required to reduce the number of exploitable weaknesses, sensor networks to detect the presence of malicious software or malicious user behavior, and various identity management and authentication frameworks to facilitate the application of access control technologies to software, data and users.

A key enabler in protecting both the local and national aspects of a Smart Grid is defining a comprehensive methodology through which the trustworthiness of devices used within the grid can be established. Trusted Computing environments provide a base platform to perform cryptographic operations to manage identity and authentication, and thus trust, but were not developed to provide end-to-end security for heterogeneous environments [13]. Summarising the content of various statements made by senior staff at the U.S. National Institute of Standards and Technologies (NIST) [4], there exists a gap between today's CKM/public key infrastructure and the requirements needed to vastly improve ICT security. To this end, in 2009 NIST called for new designs that are highly available, fault tolerant and secure against destructive attacks [4].

Other work involves considering Trusted Computing within the context of provenance - the notion that the history of data can be maintained and verified [17]. Although it can be argued that Trusted Computing is a step in the right direction (despite its controversial nature), it does not immediately solve the problem of securing a distributed system like that of a Smart Grid.

Hence, we note the existence of a gap between the notion of trust that considers object identity, and that which incorporates object behavior. But the challenge in deriving a more comprehensive view of trust (and ultimately risk) from network behavior is that it is inherently subjective when compared to electronic identities. Trust can be viewed as a layered concept that is realized by a number of perspectives that include an object's identity and behavior.

Behavioral trust adds a historical context to a static assertion checking model. This history can be used to determine if the software, hardware or user performing an action has a known dirty track record and is considered a high security risk. What large systems need are formal strategies to derive trust from new online global identity management and cryptographic key management IdM/CKM architectures, such as the proposal from Synaptic Laboratories [10] that satisfies many of NIST's 2009 CKM requirements, and by creating and synergistically integrating a dynamic notion of trust derived from Network Behavioral Analysis (NBA). Behavioral-based trust has been researched as a enabling technology to provide trust in an open environment such as NNEC [23, 13].

In this paper we explore the trustworthiness of devices in pervasive networks, as derived from both object identity and object behavior, and then attested using a distributed decentralized notion of trust. We define a behavioral-based trust of hosts that is derived from aggregated network behaviors, which offers a model to bridge the gap between object identity and behavior, and thus provide a layer of trust that can be used in open environments [19]. This approach is rooted in the context of a global/enterprise IdM/CKM system, thus offering an extension to trust for open computing environments [10]. We have applied this concept notional for NATO's NAF infrastructure [18].

In Section 2, we identify the types of threats that systems face. We provide a more descriptive notion of trust in Section 3, followed by a layered methodology in Section 4. We conclude in Section 5.

2. WHAT IS THE THREAT?

The complexity of cyber threats has steadily increased in recent years, as has the vulnerability of our information and communication technology with their ongoing reliance on international systems with system wide single point of trust failures [22]. This has immense implications for Smart Grid technology, since the level of automation will necessarily increase, resulting in increased risk due to the unpredictability of attackers – not to mention known vulnerabilities [2].

We have already noted the use of SCADA systems within a Smart Grid environment. Ongoing assessments show that there are significant vulnerabilities that have yet to be addressed (and which are not made public for obvious reasons). One estimate suggests that 12% of approximately 15 new threats each day apply to such systems [20].

The fact that the increased use of Smart Grid technology implies an increased reliability on the Internet brings its own set of weaknesses, since network protocols each have their own set of vulnerabilities. These are in addition to the security risks that are inherent in increased automation and SCADA control systems, and not to mention security risks involved in the increase use of wireless networks. Also, Smart Grid is reliant upon the legacy power grid, thus known vulnerabilities in that domain still apply. It is no secret that introduction of other supporting technologies will increase security risk [2].

The following quote from [2] sums up the threat succinctly:

> Consider the potential consequences of a successful cyber attack on the Smart Grid network. Many compromised Smart Meters or data collector nodes could be programmed by the attacker to simultaneously send messages that cause power demand to be reduced dramatically and then to be increased dramatically. These phony messages could cause grid instability and power outages.

Our purpose here is not to comprehensively survey the Internet threat landscape, but to flag that it is becoming increasingly difficult to defend against today's complex threats without defensive capabilities that can perceive behaviors operating over long time periods (e.g., months and years). For example, a single bot in a botnet has a known lifecycle that is difficult to detect with conventional means [16].

3. WHAT IS TRUST?

A large number of trust models have been created, most of which define trust statically, i.e., in terms of the identity and authentication of single entities within a network information system. These "fixed evaluation schemes contradict the subjective nature of trust" and the operational needs and vulnerabilities inherent in open systems [23]. Even though a system can be identified and authenticated by cryptographic means, it still can be compromised by threats like a botnet. Open and heterogeneous computing environments need a more dynamic formalization of trust, combined with trust derived from identity.

In [17], Martin *et al.* presents a strong case for a "trusted provenance." A key enabler for this concept is the recording of provenance information providing metrics and assurances associated with the trustworthiness of a system. The paper leverages standards associated with Trusted Computing to enforce trustworthy behavior developing a "chain of

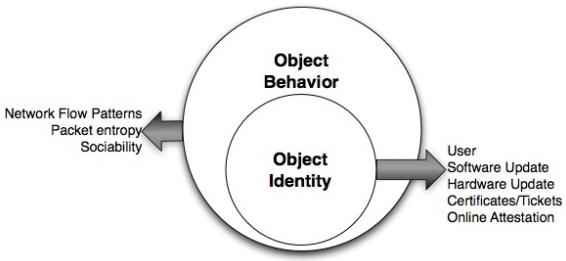

Figure 1: A Layered Notion of Object Trust

trust" through audits done on software and hardware [3]. Dasgupta has studied immune signaling mechanisms and modeled their application to cyber defense technology [6]. Forrest *et al.* applied the Biological Immune System (BIS) concepts of "self, non-self" to computer security by detecting abnormal Unix processes on a host [9].

Instead of comparing the human bodies BIS as an analog to a single host, perhaps we could view the human body as a set of independent entities (e.g., cells) coming together to form self. The digital analog of a BIS can then be the application of "self, non-self" to a complex network of devices, where signaling is not only found within the device (e.g., hosts, PLC), but also across devices connected within a network (e.g., ECS). Trust, from the perspective of the Smart Grid, can then be seen as a metric used to determine self from non-self. Trust can be derived from various methods of signaling within a multi-layered distributed system, where signaling can be viewed as a form of both "feedback" and "recommendations" from network devices (see Weth and Böhm [23]).

In this paper we establish a layered notion of trustworthiness combining object identity, and object behavior. We look at trust derived from object identity as closely being related to provenance information providing trust in a provenance in [17]. We define behavioral trust as a metric derived from a host's network behaviors measured by a sensor performing aggregated behavioral analysis. We look at behavioral trust as another component to be used in establishing a "trusted provenance." Lastly, we look at signaling as a mechanism in which trust is shared and measured within complex systems like the Smart Grid.

4. TRUST: DISTRIBUTED, DECENTRALIZED AND LAYERED

This section presents a derivation of trust in terms of object identity and behavior (Figure 1).

4.1 Trust in Terms of IdM/CKM

In June 2009 NIST held a Workshop on CKM. NIST identified the need for new CKM designs as part of the US National Cybersecurity Strategy. Such designs should be highly available, fault tolerant, secure against destructive attacks, scalable to billions of users/devices, be secure against quantum computer attacks and not use public key technologies. Additionally they must support accountability, auditing policy management which we observe are requirements leaning towards behavioural trust. Today, approximately 86% of fraud happens by management level staff against their own organisation [14]. Today's civilian PKI has 20+ Root Certificate Authorities, each of which are a system-wide single point of trust failure for identities on the Internet [22, 12]. Any new IdM/CKM architecture must employ redundancy to achieve high availability, fault tolerance, and survivability against destructive attacks. In this paper we assert that IdM/CKM systems should distribute the execution of each provisioned service across m autonomously owned/managed service providers to mitigate insider fraud/ attacks. We point to the m-1 secure symmetric key distribution protocol proposed in 1976 that exploits m key distribution centers [8] and Synaptic's IdM/CKM proposal which extends that result [11]. Both these architectures permit the principles of 'separation of powers' and 'checks and balances' to be embodied [7].

4.2 Trust in Terms of Device Identity

Non-repudiation is the concept of ensuring that a device cannot repudiate, or refute the validity of a statement it uttered. In practice, trusted hardware security modules, such as CPU based smart cards, are required to manage secrets known only to that device. In public key systems this is achieved by the smart card generating its own {public, private} key pair. In m-1 secure symmetric key systems this is achieved by ensuring that only the smart card has knowledge of all m secrets. If utterances are relayed through the m service providers, such utterances can be witnessed by the IdM/CKM on behalf of other users in the network.

4.3 Trust in Terms of Device Behavior

Network behavioral analysis is based on a methodology of determining normal behaviors within a given network. These behaviors can be derived from the structural patterns of network activity of these devices. Threat behavior can then be defined by deviations from the normative specification of normal behavior [15]. Network behavioral analysis has been performed using a Multi-Agent System (MAS) Camnep. This system captured and aggregated trust derived from network behaviors and shared that trust with various agents within the MAS [21]. We have shown that host aggregated behaviors are consistent over various time periods using our cyber data fusion system (i.e., Sonalysts's DMnet), and that these behaviors can be aggregated from sensors dispersed over multiple geographic regions [19]. Behavioral trust can be derived from multiple network behaviors measured for a given device. Unlike identity, the behavioral trust of a device is subjective and must closely follow the security policies of its deployed environment. Furthermore, we are currently exploring visual approaches to segmenting and understanding the n-dimensional feature space of aggregated host behaviors, with the goal of using visualization to provide insight into behavioral regions, and thus promoting the discovery and definition of traffic-narratives. The notion of a traffic-narrative was presented at the most recent offering of FloCon [5].

4.4 A Layered Trust Methodology

Let us consider the scenario of remote malware detection. Behavioural information about a IP address is stored in a distributed decentralized fashion within a sensor network run by several autonomous providers. Information about abstract network access behaviour is traded without initially exposing IP address information. After a threat

behaviour has been identified, sensor providers can opt to exchange information about at-risk IP addresses to confirm the threat. Once a sensor network has reached agreement about a threat, a method of notifying the community and the compromised hosts is required. In an online global IdM/CKM system based on symmetric key techniques, tokens must log-in to access services. The tuple {token, time, date, IP address} can be stored by a global IdM/CKM system allowing for reverse look-up of tokens to IP address access periods. The sensor networks can send notification requests to the global Idm/CKM system which routes the request using reverse look up. In this way, remote detection of certain classes of malware can lead to notification to users/administrators/ISP and then remedial action.

5. CONCLUSIONS

We must look beyond conventional "point source" and single vendor cyber defense strategies when providing end-to-end security for emerging complex networks like the Smart Grid, and thus foster the development of distributed defensive strategies. In order to realize these strategies, a set of enabling technologies and supporting operations are needed. Considering the complexity of Smart Grids, we note that there is no single strategy that can deter such a wide range of known and emergent threats. In this paper we explored the trustworthiness of devices in pervasive networks that is derived from both object identity and object behavior.

6. ACKNOWLEDGMENTS

Sonalysts would like to acknowledge support from of the Cyber Security Program Area of the Command, Control and Interoperability Division within the Science and Technology Directorate of the U.S. Department of Homeland Security, especially the support from Dr. Douglas Maughan. We acknowledge the efforts of the National Cyber Leap Year 2009 organizers in providing the Co-Chairs Report [1]. Joel Glanfield gratefully acknowledges the support of NSERC.

7. REFERENCES

[1] National cyber leap year reports. at `http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf`.

[2] Study of security attributes of smart grid system current cyber security issues. Paper., DOE - National SCADA Test Bed, 2009.

[3] Trusted computing homepage, 2010. Available at `https://www.trustedcomputinggroup.org/home`.

[4] E. Barker, D. Branstad, S. Chokhani, and M. Smid. Cryptographic key management workshop summary (draft). Interagency Report 7609, NIST, June 2009.

[5] M. Collins. Flow traffic analysis narratives, 2010. `http://www.cert.org/flocon/2010/flocon2010_abstracts.pdf`.

[6] D. Dasgupta. Immuno-inspired autonomic system for cyber defense. *information security technical report 12*, 2007.

[7] B. d. M. de Secondat, Charles. *The Spirit of the Laws*. Crowder, Wark, and Payne, 1777.

[8] W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. In *AFIPS '76*, pages 109–112, New York, NY, USA, June 1976. ACM.

[9] S. Forrest, P. Alan S, L. Allen, and R. Cherukuri. Self-nonself discrimination in a computer. *IEEE Symposium on Security and Privacy*, 1994.

[10] B. Gittins and R. Kelson. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without PKC: slideshow. In *IEEE Key Management Summit 2010*, Lake Tahoe, Nevada on May 4-5, 2010., May 2010. IEEE. (To Appear).

[11] B. Gittins and R. Kelson. Part 2 of SLL input to THINK-TRUST's consultation on their draft "3.1B Recommendations Report" to the European Commission. Technical report, Synaptic Laboratories Limited, www.synaptic-labs.com, January 2010. at `http://media.pqs.io/pub/papers/TT/20100126-TT-D3-1b-P2.pdf`.

[12] P. Gutmann. *Engineering Security*. (draft book), Dec. 2009.

[13] V. Haldar and M. Franz. Symmetric behavior-based trust: a new paradigm for internet computing. In *NSPW '04: Proceedings of the 2004 workshop on New security paradigms*, pages 79–84, New York, NY, USA, 2004. ACM.

[14] KPMG. Profile of a fraudster survey 2007. Forensic advisory, KPMG International, Apr. 2007. Available at `http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf`.

[15] S. Y. Lim and A. Jones. Network anomaly detection system: The state of art of network behaviour analysis. pages 459–465, 2008.

[16] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang. Botnet: Classification, attacks, detection, tracing, and preventive measures. *EURASIP Journal on Wireless Communications and Networking*, 2009.

[17] J. Lyle and A. Martin. Trusted computing and provenance: Better together. *TAPP 2010 Workshop on the Theory and Practice of Provenance*, 2010.

[18] O. McCusker, J. Glanfield, S. Brunza, C. Gates, J. McHugh, and D. Paterson. Combining trust and behavioral analysis to detect security threats in open environments. Technical report, NATO/OTAN, 2010.

[19] O. McCusker, A. Kiayias, D. Walluck, and J. Neumann. A combined fusion and mining strategy for detecting botnets. In *CATCH '09: Proceedings of the 2009 Cybersecurity Applications and Technologies Conference for Homeland Security*, 2009.

[20] M. McQueen, W. Boyer, T. McQueen, and S. McBride. Empirical estimates of 0day vulnerabilities in control systems. pages 6-1–6-26, 2009.

[21] M. Rehak, M. Pechoucek, M. Grill, J. Stiborek, K. Barto, and P. Celeda. Adaptive multiagent system for network traffic monitoring. *IEEE Intelligent Systems*, 24(3):16–25, 2009.

[22] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. M. M. de Weger. Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In *CRYPTO '09*, volume 5677 of *LNCS*, pages 55–69, Berlin, Heidelberg, Aug. 2009. Springer-Verlag.

[23] C. V. D. Weth and K. Böhm. A unifying framework for behavior-based trust models, 2006.