Next Generation SCADA Security: Best Practices and Client Puzzles

(Calvert L. Bowen, III, Timothy K. Buennemeyer, and Ryan W. Thomas)

Bradley Department of Electrical & Computer Engineering
Virginia Polytechnic Institute & State University

Presentation By

LTC Calvert L. Bowen, III and
LTC Timothy K. Buennemeyer

SCADA Hacking Report (11 March 2005)

MSNBC.com

Hackers target U.S. power grid

Government quietly warns utilities to beef up computer security

By Justin Blum
The Washington Post
Updated: 8:33 a.m. ET March 11, 2005

WASHINGTON - Hundreds of times a day, hackers try to slip past cyber-security into the computer network of Constellation Energy Group Inc., a Baltimore power com… …omers around the country.

"V… …llins, chief risk officer for Constellation, which operates Baltimore Gas and Electric. "We just know it's being hit."

H… …ir untiring efforts have heightened concerns that electric companies have failed to adequately fortify d… …orists or others could engineer an attack that sets off a widespread blackout and damages power plants, prolonging an outage.

Pa… …eeting in January that they need to focus more heavily on cyber-sec… …tential terrorist strike, but Wood stepped up his campaign after officials at…

Wood declined to comment on specifics of what he saw. But an official at the lab, Ken Watts, said the simulation showed how someone could hack into a utility's Internet-based business management system, then into a system that controls utility operations. Once inside, lab workers simulated c…

Describing his reaction to the demonstration, Wood said: "I wished I'd had a diaper on."

Hundreds of times a day, hackers try to slip past cyber-security into the computer network of Constellation Energy

Chief Risk Officer:
"We just know it's being hit."

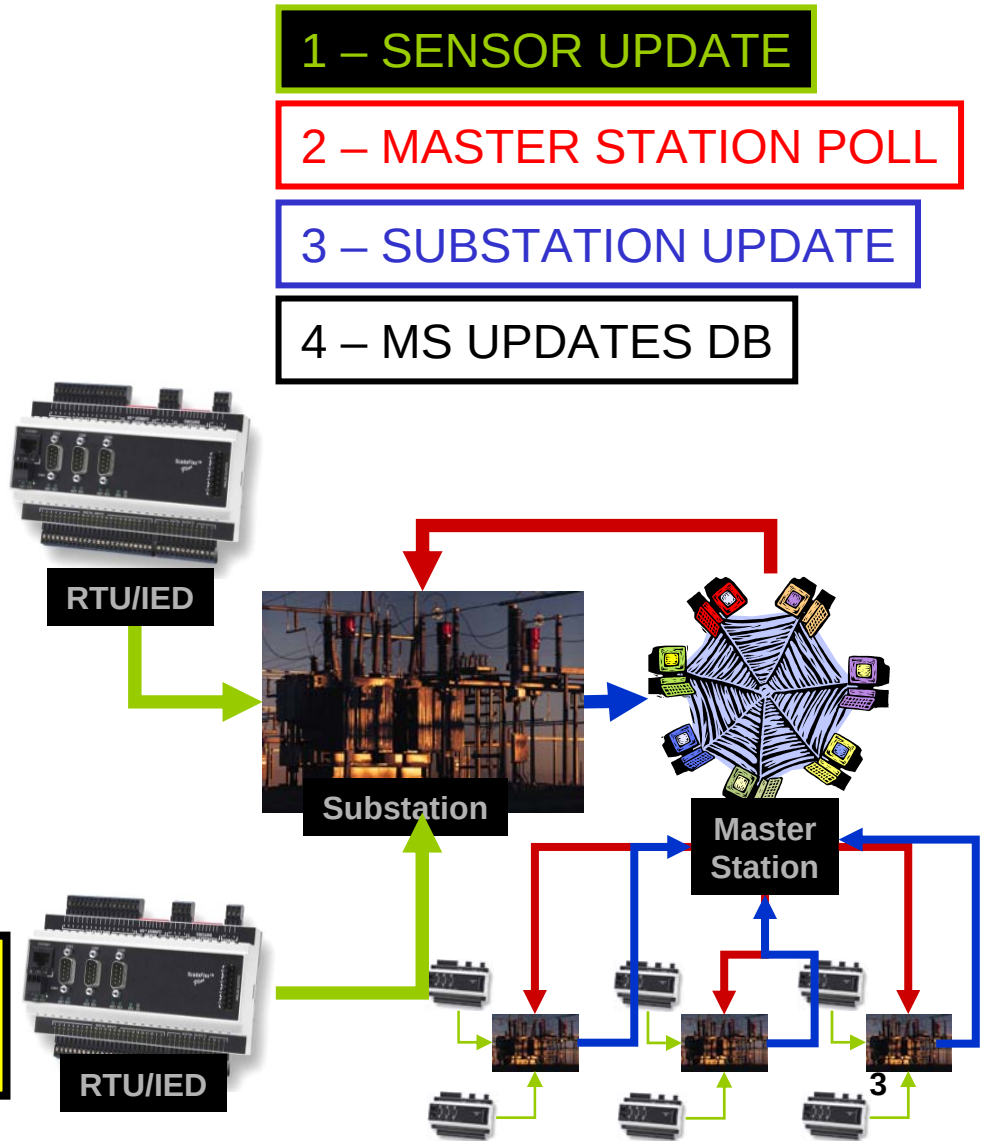
In a worst-case scenario, terrorists…could engineer an attack that sets off a widespread blackout and damages power plants…

…someone could hack into a utility's Internet-based business management system, then into a system that controls utility operations.

Chairman, Fed Energy Regulatory Commission:
"I wished I'd had a diaper on."

SCADA Communication System

- Primitive Compared to Most Modern Networks
- Proprietary Hardware & Software (Past)
  - Manuals & Procedures Not Widely Available
  - Closed Systems Considered Immune to Outside Threats
- Networks Becoming Interconnected (Today)
  - Utility Networks, Corporate Networks (Intranets), Internet
  - DNP3 rides on top of TCP/IP
- Susceptible to SYN Flood attacks aimed at Substations



SCADA Security Problem

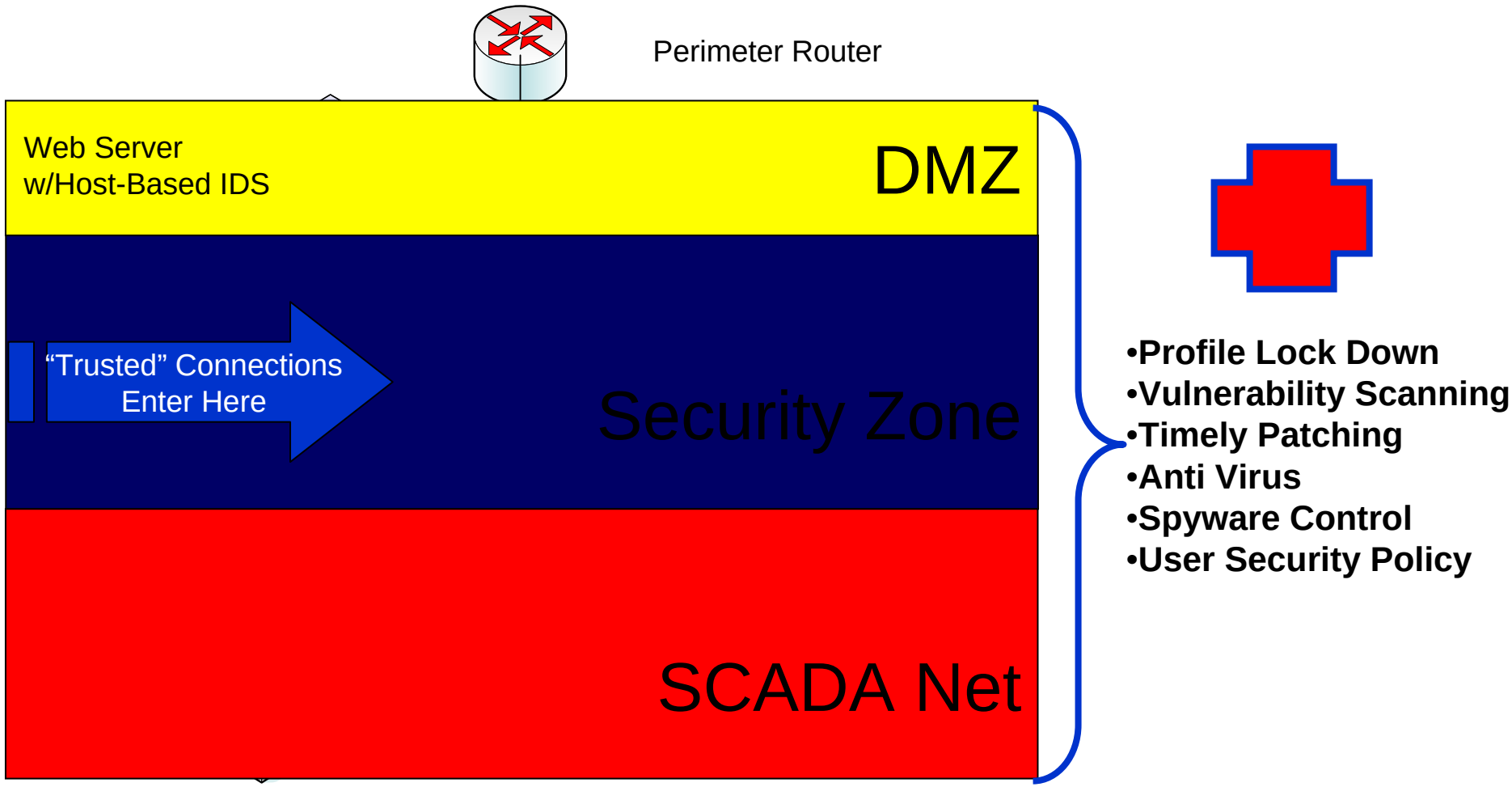
- SCADA Network Vulnerabilities Unveiled
  - Internet Connection = Cyber Attacks Now Possible
  - Common Operating System Vulnerabilities Exposed
  - Legacy and Newer Equipment Incompatibilities
  - Online Protocol Libraries & System Documentation
- Electrical Power Utility Deregulation
  - Competitive Industry
  - Security & Network Upgrades = Higher Costs
- Physical Threats
  - Insider Threats
  - Terrorist Threats (Heightened After 9-11 Attacks)
  - Nation State Level Threats

Next Generation SCADA Security

- Establish A Defense in Depth Architecture
  - Reverse current network integration trends
  - Isolate SCADA systems from general network access
  - Provide Information Assurance and Data Integrity

- Defensive Layers
  - Multiple Firewalls and Proper IP Masking on Private Networks
  - Employ DMZ located Web Servers for common data visualization
  - Employ network and host based IDS monitoring
  - Eliminate unnecessary processes & close used ports
  - Conduct timely system software patching
  - Advocate user security awareness policy

Best Practices: Defense in Depth



Assumptions and Scenario

ASSUMPTIONS

- Connections do (and will continue to) exist between SCADA networks and corporate or external networks
- Next generation SCADA systems will use TCP for transport protocol and COTS platforms and media
- Access to the sensors is only through the SS
- SSs are the target of the DoS based on the polling requests from the MS
- Protection Event messages have mechanism to override any current connection

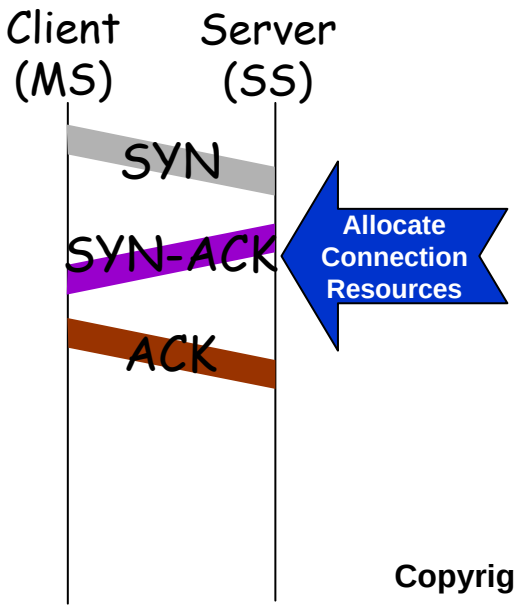
SCENARIO

- Regional Power Provider
- Best Practices NOT Fully Implemented
  - SCADA Net Exposed & Vulnerable to Exploits
  - Attack Vector is TCP SYN Flood
- Target—Substation Server
- Attack Goal—Disrupt SS to MS Data Updates
- Intension—DoS Against SS to Delay MS Control OPNS

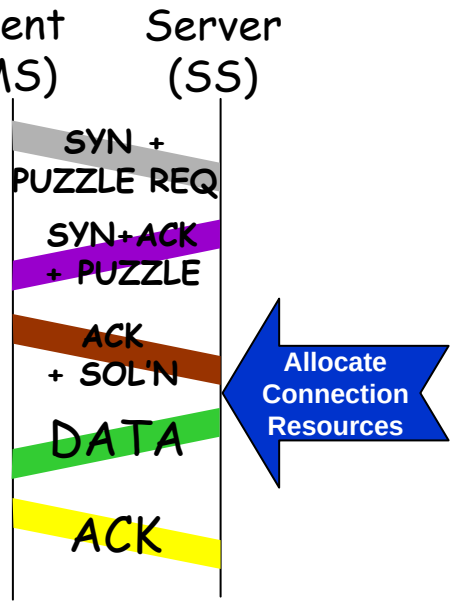
How Client Puzzles Work

- TCP uses a “3-way” handshake (SYN, SYN+ACK, ACK)
- But there is a flaw in this scheme:
  - Flooding with SYN packets
  - Creates numerous “Half-Open” connections
  - System crashes when SYN Queue overflows at 4,096 bytes
- Client Puzzles change the connection protocol asymmetry

Standard TCP



pTCP

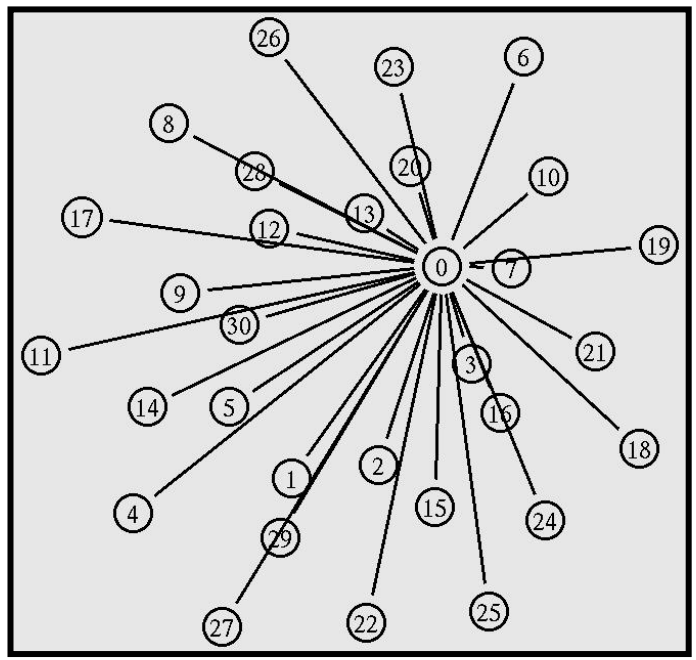


SCADA Quality of Service

- Benchmarks for SCADA Power Generation Systems
- Substations per Master Station = 30
- Sensors per Substation = 47
- Response Requirements:
  - Protection Event 0.004 sec
  - SCADA Transactions 0.540 sec ← Latency Focus
  - Fault Records 600.000 sec
- SCADA messages are very small <1,000 bits
- Expect 47,000 bits per Substation to Master transaction
- Updates are randomly distributed from 20-60K bits
- Polling for updates at 2 sec intervals

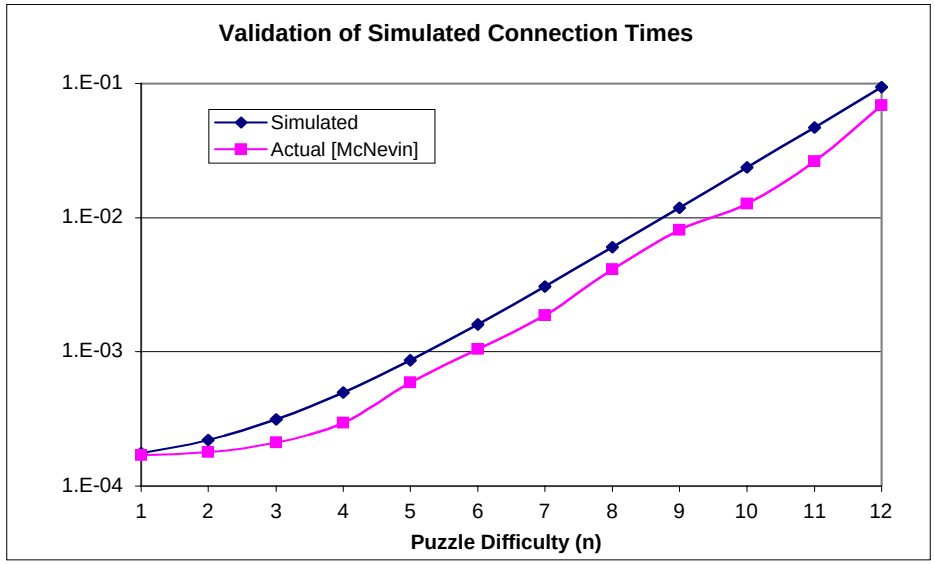
Simulation

- ns2
  - implements pTCP as discrete event simulator
  - Creates stacks of events that spawn more events
  - Focus of simulation was master station (MS) to substation (SS) delay
  - Mirrors the “round robin” polling by MS to SS
- Setup
  - Modified standard TCP package
  - # nodes: 1 MS, range of SS (2 to 100)
  - Message Length: random distribution between 20k-60k bits
- 49 Experiments – 7 Puzzle Difficulties, 7 Node Counts



Simulation & Results

- Concerned about Message Delay compared to Puzzle Difficulty
- Simulation closely equates to actual measured results



- Time to solve Puzzle = $2^n * T$
- Normalized Puzzle Difficulty to account for CPU speed:

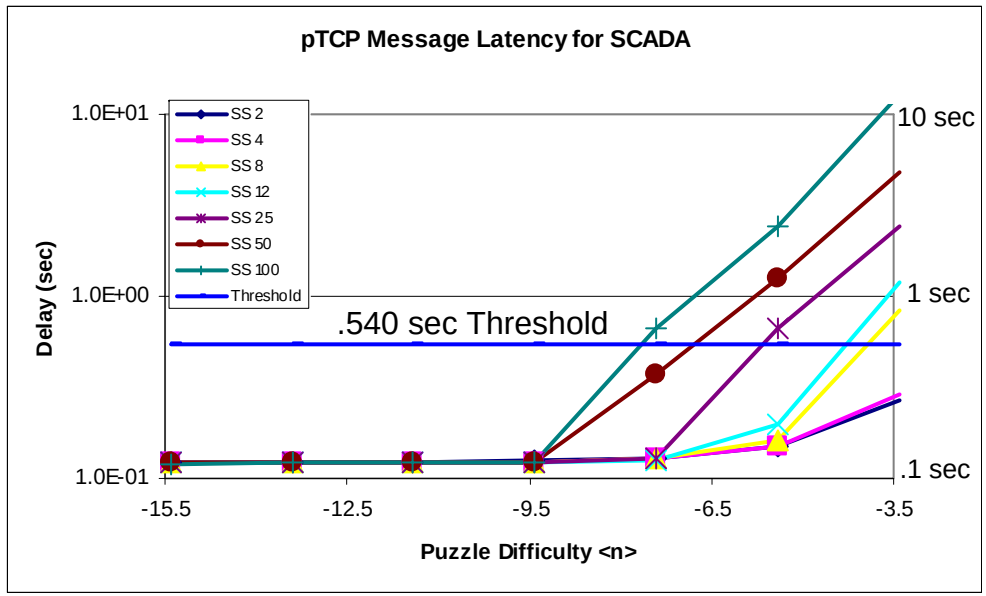
$$\langle n \rangle = \log_2(T) + n$$

  - T = Time to Run an eXtended Tiny Encryption Algorithm (XTEA6)
  - n = Puzzle Difficulty

ns-2 Observations & Results

- 49 ns-2 scenarios run
- Results show latency increasing over time
- pTCP is feasible if normalized puzzles are ≤ level -9.5
- Puzzle difficulty increases as DoS attack builds
- Puzzle difficulty inhibits attacker by draining computational resources

# SS	Delay at <*n*> =		
	-9.5	-7.5	-5.5
2	0.1248	0.1295	0.1484
4	0.1229	0.1275	0.1508
8	0.1231	0.1276	0.1612
12	0.1224	0.1269	0.1966
25	0.1224	0.1272	0.6594
50	0.1225	0.3683	1.2527
100	0.1226	0.6612	2.4358



References

1. Beaver, C. L., Gallup, D. R., NeuMann, W. D. and Torgerson, M. D., “SAND Report: Key Management for SCADA” (SAND2001-3252), Sandia National Laboratories, 2002, Albuquerque, New Mexico, USA.
2. Bruce, A.G., Lee, R., “A Framework for the Specification of SCADA Data Links”, IEEE Transactions on Power Systems, Vol. 9, No. 1, 1993, USA.
3. CERT/CC, “Attack Trends”, (www.cert.org/archive/pdf/attack_trends.pdf), 2002, USA.
4. Curtis, K.A., “DNP3 Protocol Primer”, DNP Users Group, (www.dnp.org/files/dnp3_primer.pdf), 2000, USA.
5. EPRI, Destinations 2004, “Project 86: P86.005 Development of Security for Distribution Automation and SCADA Systems”, (www.epri.com/D2004/dilbert.aspx?id=743&year=2004), 2004, USA.
6. EPRI, Destinations 2005, “Project 86: P086.002 Security for Distribution Automation and SCADA Systems”, (www.epri.com/destinations/product.aspx?id=368), 2004, USA.
7. Fall, K., and Varadhan, K., “ns Manual”, (www.isi.edu/nsnam/ns/doc/ns_doc.pdf), 2004, USA.
8. Forouzan, B.A., TCP/IP Protocol Suite, McGraw Hill, 2000, pp. 293-299, USA.
9. Jones, D.A., “Security”, IEEE Spectrum, June 1999, pp 47-48, New York, NY, USA.
10. Killcrece, G., Kossakowski, K.P., Ruefle, R., Zajicek, M., “State of the Practice of Computer Security Incident Response Teams (CSIRTs)”, Technical Report (CMU/SEI-2003-TR-001), (www.cert.org/archive/pdf/03tr001.pdf), October 2003, Pittsburgh, PA, USA.
11. McCanne, S. and Floyd, S., “ns Network Simulator”, (www.isi.edu/nsnam/ns/), 2004, USA.
12. McDonald, John D., Electrical Power Substations Engineering, CRC Press, 2003, New York, NY, USA.
13. McNevin, T.J. and Park, J.M., “pTCP: A Client Puzzle Protocol For Defending Against Resource Exhaustion Denial Of Service Attacks” (Draft), Unpublished Manuscript, 2004, USA.
14. Pollet, J., “Developing a Solid SCADA Security Strategy”, [Conference Paper] SIcon/02. Sensors for Industry Conference, Proceedings of the ISA/IEEE. (IEEE Cat. No. 02EX626), 2002, pp 148-56, Research Triangle Park, NC, USA.
15. Skoudis, E., Counter Hack, Prentice Hall, 2002, Upper Saddle River, NJ, USA.
16. Su, C.L., Lu, C.N., Hsaio, T.Y., “Simulation Study of Internet Based Inter Control Center Data Exchange for Complete Network Modeling”, IEEE Transactions on Power Systems, Vol., 17, No. 4, 2002, USA.
17. Weiss, J., Personal Communication, 8 OCT 2004.
18. Wheeler D., and Needham R., “TEA Extensions” (Draft), Unpublished Manuscript, (www.cl.cam.ac.uk/ftp/users/djw3/xtea.ps), 2004, USA.

Biographies

- **LTC Calvert L. Bowen, III** is a career US Army Officer. He is currently a PhD student at Virginia Tech. His research interests include computer/network security, access control and context awareness. His education includes an MS in Computer Based Systems Engineering from George Mason University, and an MBA from the University of Hawai'i. As the Chief of Theater Information Assurance for US forces across the Pacific Theater, he was a key member of the Computer Network Defense Cell which was selected as Federal Executive Board's 2004 Pacific Region Organization of Excellence. He is a student-member of IEEE. (triiip@vt.edu)

- **LTC Timothy K. Buennemeyer** is an active duty US Army Officer and PhD student at Virginia Tech. His research interests include network security, ad hoc sensor networks, and context aware systems. He earned his MA in Computer Information Management in 1998 from Webster University. As the US Pacific Command Division Chief for Computer Network Defense and Information Assurance, he managed Headquarters cyber defenses and system accreditation programs. His team won the Federal Executive Board's 2004 Pacific Region Organizational Excellence Award, and he won the National Security Agency's 2004 Frank B. Rowlett Information Assurance Award for individual achievement. He is a member of the Armed Forces Communication Electronics Association. (timb@vt.edu)

- **Capt Ryan W. Thomas** is an active duty US Air Force officer and PhD student at Virginia Tech. His research interests include network security, access control and quality of service. He was previously assigned to the Air Force Research Laboratory, Sensors Directorate as a developmental engineer. Captain Thomas received his Masters degree in 2001 from the Air Force Institute of Technology. (rwrthomas@vt.edu)